Лекция 7. Сетевая безопасность

Содержание

- Сетевая безопасность – проблемы, механизмы, сервисы
- Фильтрация пакетов
- Межсетевые экраны
- Системы обнаружения и предотвращения вторжений
- Системы анализа трафика
- Системы обнаружения и предотвращения атак
- Защита от DDoS-атак
- Шлюзы информационной безопасности
- Криптошлюзы

- **Сетевая безопасность** — это инструменты, тактика и политика безопасности для мониторинга; предотвращения и реагирования на несанкционированное проникновение в сеть; защиты цифровых активов и сетевого трафика. Киберпреступность неустанно растет, и организациям требуются аппаратные и программные технологии для борьбы с угрозами и предоставления видимости сети.
- Сетевая безопасность предназначена для реагирования на потенциальные угрозы в компьютерной сети, и включает следующие уровни:
- Защита электронной почты и серверов.
- Защита серверов.
- Защита данных.
- Мобильная безопасность.
- Защита сети.
- Приложение облачных сервисов.

- **Сетевые угрозы**, незаконные или вредоносные действия, направлены на использование уязвимостей в сетях, серверах и доступах. Цель злоумышленников – взломать, нанести вред или саботировать ценные данные.
- **Стратегия сетевой безопасности** должна учитывать сектор и методы, с внедрением которых поможет системный интегратор. Правильный подход включает не только использование безопасности сетевого уровня. Решения по сетевой безопасности экономят время и средства, улучшают локальные и другие операции, повышают соответствие требованиям и минимизируют повреждения данных.

Сетевая безопасность
Проблема безопасности

- В отсутствии защиты компьютерная сеть подвержена сетевым атакам самого различного типа
  - Прослушивание (sniffing) – перехват передаваемой по сети информации
  - Наличие посредника (man-in-the-middle), способного просматривать содержимое трафика и изменять его
  - Подделка источника (spoofing) – передача данных от чужого имени
  - Компрометация пользователя – получение идентификационной информации пользователя, возможность доступа к ресурсам от его имени
  - Отказ в обслуживании (denial of service, DOS) – перегрузка или блокирование сервиса
  - …

Сетевая безопасность
Общие термины

- Компрометация – действия, в результате выполнения которых объект компрометации становится небезопасным
  - Получения имени и пароля учетной записи пользователя сторонним лицом – компрометация учетной записи
  - Изменение передаваемых данных – компрометация данных
- Атака – действие, направленное на компрометацию какого-либо объекта
- Уязвимость – (слабое) место в системе (аппаратное или программное), которое может быть атаковано
- Механизм безопасности – аппаратное или программное средство, защищающее уязвимости от атак
- Политика безопасности – порядок защиты информации в организации (контролирует порядок хранения, обработки и обмена информацией)
- Сервис безопасности – комплекс аппаратных и программных средств, реализующих политику безопасности

Сетевая безопасность
Сервисы безопасности

- Защита от повторений (replay prevention) – обеспечивает уникальность каждого сообщения
  - Например, можно для каждого IP-пакета указывать уникальный номер с момента последней смены ключей в установленном соединении
  - Требуется для того, чтобы узел, который мог получить передаваемый пакет, не смог воспользоваться им впоследствии для установления сеанса с получателем
- Контроль доступа – позволяет ограничить и контролировать доступ к ресурсам

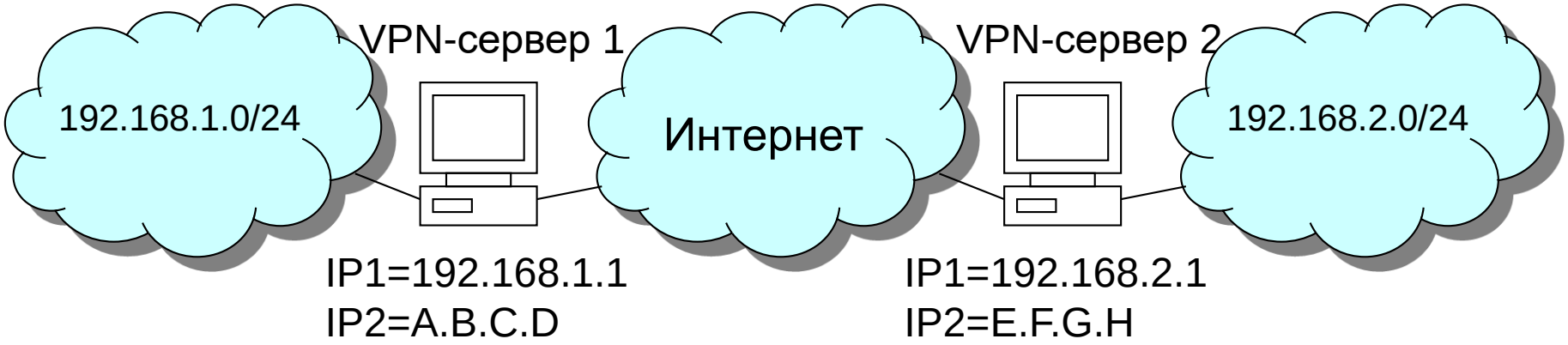
Сетевая безопасность IPSec

- IPSec (IP-Security) – IP-безопасность, основана на защите соединений "точка-точка" и реализует
  - защиту IP-пакетов
  - защиту от сетевых атак
- Использует протоколы
  - Encapsulated Security Payload (ESP) - защита данных IP-пакета путем шифрования содержимого с помощью симметричных криптографических алгоритмов (Blowfish, 3DES).
  - Authentication Header (AH) – защита заголовка IP-пакета путем вычисления криптографической контрольной суммы и хеширования полей заголовка IP пакета защищенной функцией хеширования
- Безопасное соединение (Security Association, SA) – базовое понятие IPSec, означающее однонаправленное (симплексное) логическое соединение, создаваемое для обеспечения безопасности
- Используется для непосредственного шифрования трафика между двумя хостами (транспортный режим) или для построения "виртуальных туннелей" между двумя подсетями (туннельный режим)
  - Последний случай обычно называют виртуальной частной сетью (Virtual Private Network, VPN)

Сетевая безопасность Virtual Private Network…

- Описание ситуации
  - Имеется две сети
  - Внутри обеих сетей используется протокол IP
  - Сети имеют маршрутизаторы, соединенные друг с другом через Интернет
  - У маршрутизатора каждой из сетей есть как минимум один публичный IP-адрес
  - Внутренние IP-адреса сетей могут быть публичными или приватными (не имеет значения); на маршрутизаторах может работать сетевое преобразование адресов (Network Address Translation, NAT)
  - Внутренние IP-адреса двух сетей не должны пересекаться
- Необходимо организовать защищенную передачу данных между сетями через Интернет

Сетевая безопасность
Virtual Private Network



- Все пакеты, приходящие на VPN-сервер1 из сети 192.168.1.0/24 и направленные в сеть 192.168.2.0/24, инкапсулируются в пакеты ESP и отправляются через Интернет VPN-серверу2, который их извлекает и доставляет в сеть 192.168.2.0/24

Фильтрация пакетов

Фильтрация пакетов

- Фильтрация пакетов обычно делается на сетевом или транспортном уровне
  - каждый пакет проверяется на удовлетворение ряду условий
  - в зависимости от выполненных условий производится обработка пакета
- Фильтрация пакетов может выполняться на любом узле, но обязательно должна использоваться на маршрутизаторах, пограничных с Интернет
- Мы рассмотрим частный случай – фильтрация IP-пакетов посредством iptables (механизм фильтрации, реализованный в ядрах версий 2.4 и 2.6 ОС Linux)

Пакетный фильтр iptables
Признаки фильтрации

- iptables может анализировать
  - IP-адрес источника, IP-адрес получателя
  - Тип протокола
  - Номер порта источника, номер порта получателя (для протоколов TCP и UDP)
  - Флаги протокола TCP
  - Данные заголовка IP пакета
  - Признак того, что пакет является первым в последовательности
  - Другие параметры
- iptables не анализирует данные пакета

Пакетный фильтр iptables
Фильтрация

- iptables при фильтрации использует последовательности (цепочки, chains) правил, каждое из которых содержит
  - набор условий
  - выполняемое действие
- Правила в цепочке просматриваются последовательно
  - Если условия применимы к обрабатываемому пакету, выполняется указанное в правилах действие
    - В зависимости от действия просмотр правил в цепочке завершается либо продолжается
  - Если условия не применимы к обрабатываемому пакету, переходим к следующему правилу в цепочке

Пакетный фильтр iptables
Цепочки

- Поддерживается 5 встроенных цепочек
  - 1 – PREROUTING
  - 2 – FORWARD
  - 3 – POSTROUTING
  - 4 – INPUT
  - 5 – OUTPUT
- Можно создавать пользовательские цепочки, но их использование явно определяется в правилах встроенных цепочек

Пакетный фильтр iptables Таблицы…

- Для различных типов обработки IP-пакетов существуют 3 таблицы (каждая из которых имеет индивидуальный набор цепочек)
  - filter – предназначена для задания правил фильтрации пакетов;
    - 4 – INPUT
    - 2 – FORWARD
    - 5 – OUTPUT
  - nat – предназначена для задания преобразования сетевых адресов (Network Address Translations, NAT); может использовать цепочки
    - 1 – PREROUTING
    - 3 – POSTROUTING
    - 5 – OUTPUT
  - mangle – предназначена для внесения изменений в заголовки пакетов; может использовать все цепочки

Пакетный фильтр iptables
Таблицы

- При обработке пакетов порядок использования цепочек однозначно определен
  - Для транзитных пакетов
    - mangle – PREROUTING
    - nat – PREROUTING
    - mangle – FORWARD
    - filter – FORWARD
    - mangle – POSTROUTING
    - nat – POSTROUTING
  - Для пакетов, предназначенных локальному приложению
    - mangle – PREROUTING
    - nat – PREROUTING
    - mangle – INPUT
    - filter – INPUT
  - Для исходящих пакетов локальных приложений
    - mangle – OUTPUT
    - nat – OUTPUT
    - filter – OUTPUT
    - mangle – POSTROUTING
    - nat – POSTROUTING

Пакетный фильтр iptables
Утилиты

- Для управления правилами используется утилита iptables
  `iptables [opts] [-t table] [-com] [parms]`
  которая обеспечивает
  - Создание/удаление пользовательских цепочек
  - Задание политики по умолчанию для цепочки
  - Добавление/изменение/удаление правил
  - Просмотр/установку/сброс счетчиков пакетов
  - и т.д.
- По умолчанию используется таблица filter
- Утилиты iptables-save и iptables-restore позволяют сохранить конфигурацию в файл и восстановить ее из файла

Пакетный фильтр iptables Таблица filter…

- В таблице filter правила могут использовать условия отбора пакетов различных типов
  - Общие – не зависят от протокола
    - протокол
    - IP-адрес источника и IP-адрес получателя
    - входной и выходной NIC
  - Неявные – зависят от типа протокола
    - для TCP – номера портов источника и получателя и флаги TCP
    - для UDP – номера портов источника и получателя
    - для ICMP – тип сообщения ICMP
  - Явные – требуют загрузки специальных модулей
    - модуль mac позволяет проверять MAC-адреса узлов, передающих пакеты
    - модуль state отслеживает соединения между процессами и позволяет писать условия в терминах состояния соединения
    - модуль limit позволяет ограничить число срабатываний правила
    - и т.д.

Пакетный фильтр iptables
Таблица filter

- В таблице filter правила могут использовать следующие действия
  - ACCEPT – пакет принимается для дальнейшей обработки
  - REJECT – пакет уничтожается, источнику посылается ICMP-сообщение
    - Можно явно в правиле указать тип отправляемого ICMP-сообщения
  - DROP – пакет уничтожается, ICMP-сообщение источнику не посылается
  - ИМЯ_ЦЕПОЧКИ – перейти к просмотру правил указанной цепочки
  - RETURN – вернуться к просмотру правил цепочки, из которой была запрошена обработка правил текущей цепочки
  - LOG – внести запись о срабатывании правила в журнал
  - существуют другие действия

Пакетный фильтр iptables
Таблица nat

- Преобразование сетевых адресов позволяет использовать во внутренней сети адреса из частного диапазона
  - При попытке отправить пакет из внутренней сети к внешнему узлу маршрутизатор подменяет IP-адрес источника своим внешним адресом
  - При приходе ответного пакета от внешнего узла IP-адрес получателя подменяется на внутренний IP-адрес узла, пославшего исходящий пакет, и пакет передается во внутреннюю сеть
- В таблице NAT правила могут использовать следующие действия
  - SNAT или MASQUERADE – замена IP-адреса и/или порта источника
  - DNAT – замена IP-адреса или порта назначения (используется для организации доступа из внешних сетей к серверам, расположенным во внутренней сети и имеющим адреса из частного диапазона)

МЕЖСЕТЕВЫЕ ЭКРАНЫ

- Межсетевой экран (МЭ, брандмауэр или Firewall) представляет собой программно-аппаратный или программный комплекс, который отслеживает сетевые пакеты, блокирует или разрешает их прохождение. В фильтрации трафика брандмауэр опирается на установленные параметры — чаще всего их называют правилами МЭ.
- Современные межсетевые экраны располагаются на периферии сети, ограничивают транзит трафика, установку нежелательных соединений и подобные действия за счет средств фильтрации и аутентификации.


Вирусы
ПК
Межсетевой экран
Внешние атаки
Общедоступная сеть

Главная задача МЭ – это фильтрация трафика между зонами сети. Он может использоваться для разграничения прав доступа в сеть, защиты от сканирования сети компании, проведения сетевых атак. Проще говоря, межсетевой экран – это одно из устройств, при помощи которого обеспечивается сетевая безопасность компании.

Функции межсетевого экрана

Брандмауэр может:

- **Остановить подмену трафика**. Представим, что ваша компания обменивается данными с одним их своих подразделений, при этом ваши IP-адреса известны. Злоумышленник может попытаться замаскировать свой трафик под данные офиса, но отправить его с другого IP. Брандмауэр обнаружит подмену и не даст ему попасть внутрь вашей сети.
- **Защитить корпоративную сеть от DDoS-атак**. То есть ситуаций, когда злоумышленники пытаются вывести из строя ресурсы компании, отправляя им множество запросов с зараженных устройств. Если система умеет распознавать такие атаки, она формирует определенную закономерность и передает ее брандмауэру для дальнейшей фильтрации злонамеренного трафика.
- **Заблокировать передачу данных на неизвестный IP-адрес**. Допустим, сотрудник фирмы скачал вредоносный файл и заразил свой компьютер, что привело к утечке корпоративной информации. При попытке вируса передать информацию на неизвестный IP-адрес брандмауэр автоматически остановит это.

Правила МЭ

- Сетевой трафик, проходящий через брандмауэр, сопоставляется с правилами, чтобы определить, пропускать его или нет.
- Правило межсетевого экрана состоит из условия (IP-адрес, порт) и действия, которое необходимо применить к пакетами, подходящим под заданное условие. К действиям относятся команды **разрешить** (accept), **отклонить** (reject) и **отбросить** (drop). Эти условия указывают МЭ, что именно нужно совершить с трафиком:
- разрешить — пропустить трафик;
- отклонить — не пропускать трафик, а пользователю выдать сообщение-ошибку «недоступно»;
- отбросить — заблокировать передачу и не выдавать ответного сообщения.

- Для лучшего понимания рассмотрим пример. Допустим, у нас есть три правила:
- Разрешить доступ всем IP-адресам, которые принадлежат отделу маркетинга, на 80-й порт.
- Разрешить доступ всем IP-адресам, которые принадлежат отделу системного администрирования.
- Отклонить доступ всем остальным.
- Если к сети попытается подключиться сотрудник отдела технической поддержки, он получит сообщение об ошибке соединения (см. правило 3). При этом если сотрудник отдела маркетинга попробует подключиться по SSH, то также получит сообщение об ошибке, поскольку использует 22-й порт (см. правило 1).

```
FortiGate # show firewall address marketing
config firewall address
    edit "marketing"
        set uuid 728e3f24-3e29-51ec-ad86-7fd7638fda4b
        set type iprange
        set start-ip 10.0.3.1
        set end-ip 10.0.3.254
    next
end

FortiGate # show firewall policy 7
config firewall policy
    edit 7
        set name "acsess to marketing department"
        set uuid 387225d4-ac61-51ec-784d-3adea05aeba7
        set srcintf "port1"
        set dstintf "port2"
        set action accept
        set srcaddr "marketing"
        set dstaddr "all"
        set schedule "always"
        set service "HTTP"
        set logtraffic disable
    next
end

FortiGate #
```

Типы межсетевых экранов

- МЭ делятся на два основных типа: аппаратные и программные.
- Аппаратный межсетевой экран
- **Аппаратный МЭ** – это, как правило, специальное оборудование, составляющие которого (процессоры, платы и т.п.) спроектированы специально для обработки трафика.
- Работает они на специальном ПО — это необходимо для увеличения производительности оборудования. Примерами аппаратного межсетевого экрана выступают такие устройства, как Cisco ASA, FortiGate, Cisco FirePower, UserGate и другие.

Программный межсетевой экран

- **Программный МЭ** – это программное обеспечение, которое устанавливается на устройств, реальное или виртуальное.
- Через такой межсетевой экран перенаправляется весь трафик внутрь рабочей сети. К программным относятся брандмауэр в Windows и iptables в Linux.
- Программные МЭ, как правило, дешевле и могут устанавливаться не только на границах сети, но и на рабочих станциях пользователей. Из основных недостатков — более низкая пропускная способность и сложность настройки в ряде случаев.

Unified threat management, или универсальный шлюз безопасности

- Такие межсетевые экраны включают в себя антивирус, брандмауэр, спамфильтр, VPN и систему IDS/IPS (системы обнаружения и предотвращения вторжений), контроль сеансов.
- Основное преимущество данной технологии в том, что администратор работает не с парком различных устройств, а использует единое решение. Это удобно, так как производитель предусматривает централизованный интерфейс управления службами, политиками, правилами, а также дает возможность более «тонкой» настройки оборудования.

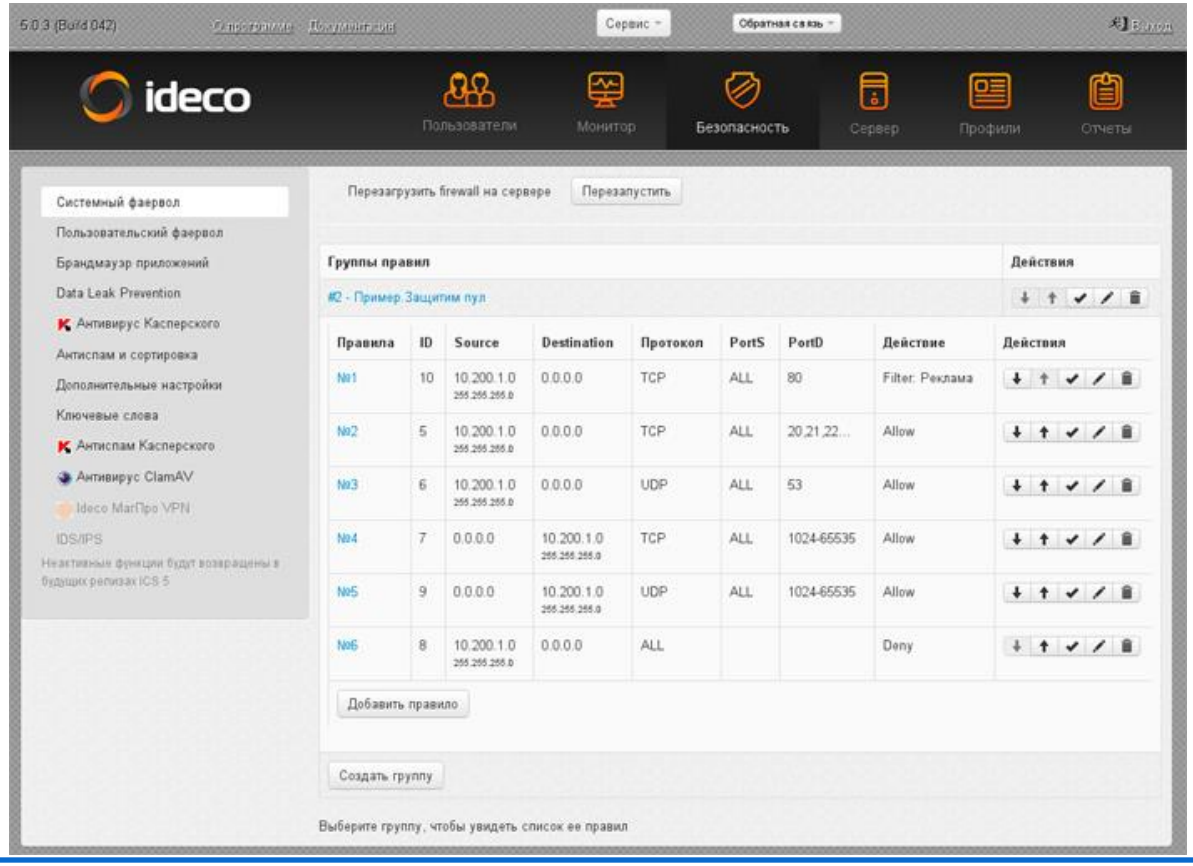
- В UTM-устройство входят несколько видов процессоров:
- процессор общего назначения, или центральный процессор,
- процессор обработки данных,
- сетевой процессор,
- процессор обработки политик безопасности.
- **Процессор общего назначения** похож на процессор, установленный в обычном ПК. Он выполняет основные операции на межсетевом экране. Остальные виды процессоров призваны снизить нагрузку на него.

- **Процессор данных** отвечает за обработку подозрительного трафика и сравнения его с изученными угрозами. Он ускоряет вычисления, происходящие на уровне приложений, а также выполняет задачи антивируса и служб предотвращения вторжений.
- **Сетевой процессор** предназначен для высокоскоростной обработки сетевых потоков. Основная задача заключается в анализе пакетов и блоков данных, трансляции сетевых адресов, маршрутизации сетевого трафика и его шифровании.
- **Процессор обработки политик безопасности** отвечает за выполнение задач антивируса и служб предотвращения вторжений. Также он разгружает процессор общего назначения, обрабатывая сложные вычислительные задачи.

Ideco UTM

- Система предотвращения вторжений
- Контентная фильтрация
- Контроль приложений

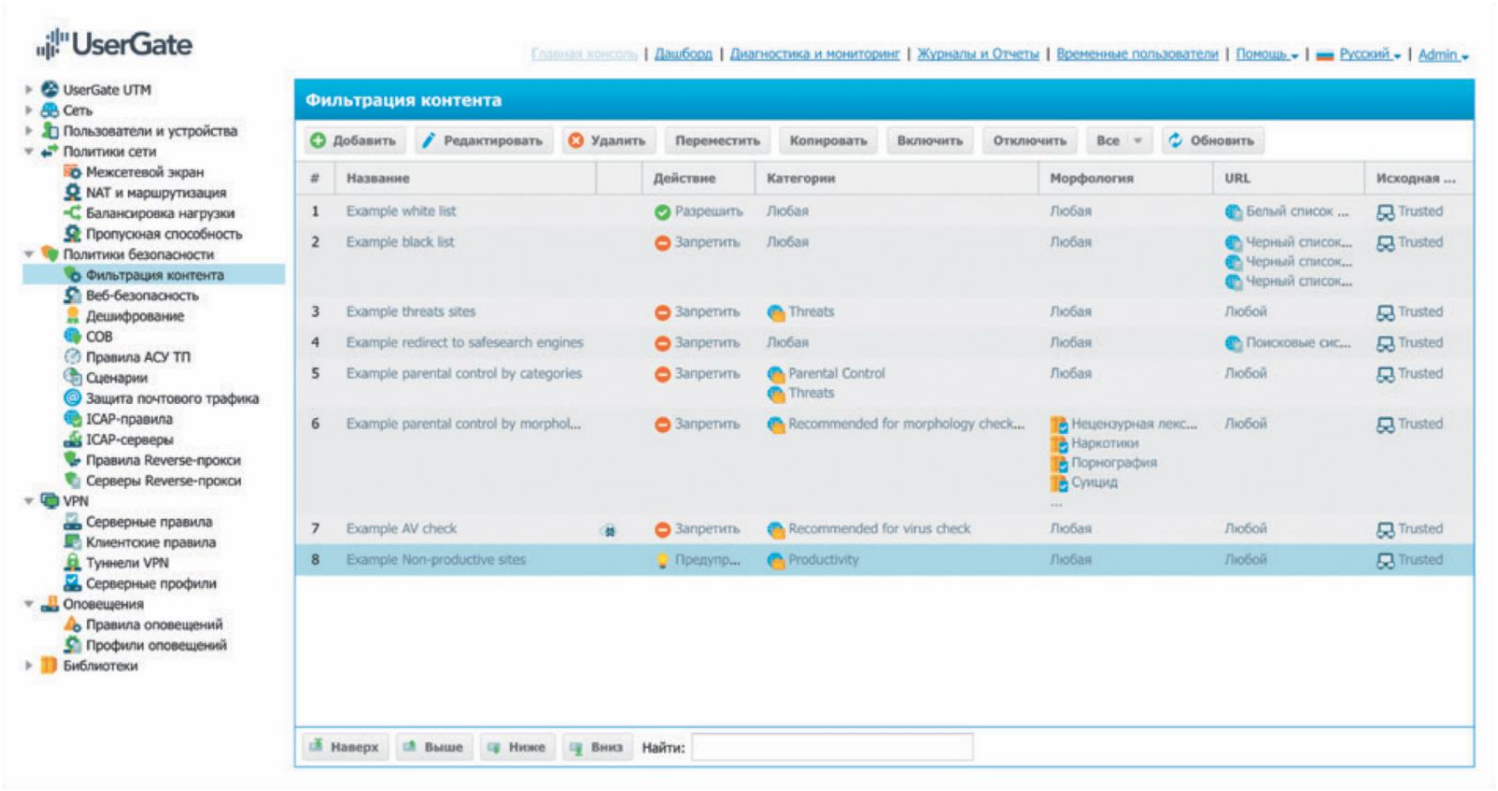
Ideco UTM


5.0.3 (Build 042)
Сервис
Обратная связь
ideco
Пользователи
Монитор
Безопасность
Сервер
Профили
Отчеты
Системный фаервол
Пользовательский фаервол
Брандмауэр приложений
Data Leak Prevention
Антивирус Касперского
Антиспам и сортировка
Дополнительные настройки
Ключевые слова
Антиспам Касперского
Антивирус ClamAV
Ideco МагПро VPN
IDS/IPS
Неактивные функции будут возвращены в будущих релизах ICS 5
Перезагрузить firewall на сервере
Перезапустить
Группы правил
Действия
#2 - Пример Защитим пул
Правила
ID
Source
Destination
Протокол
PortS
PortD
Действие
Действия
№1
10
10.200.1.0
255.255.255.0
0.0.0.0
TCP
ALL
80
Filter: Реклама
№2
5
10.200.1.0
255.255.255.0
0.0.0.0
TCP
ALL
20,21,22...
Allow
№3
6
10.200.1.0
255.255.255.0
0.0.0.0
UDP
ALL
53
Allow
№4
7
0.0.0.0
10.200.1.0
255.255.255.0
TCP
ALL
1024-65535
Allow
№5
9
0.0.0.0
10.200.1.0
255.255.255.0
UDP
ALL
1024-65535
Allow
№6
8
10.200.1.0
255.255.255.0
0.0.0.0
ALL
Deny
Добавить правило
Создать группу
Выберите группу, чтобы увидеть список ее правил

UserGate

- Поддержка АСУ ТП
- Контроль интернет-приложений L7
- Дешифрование SSL

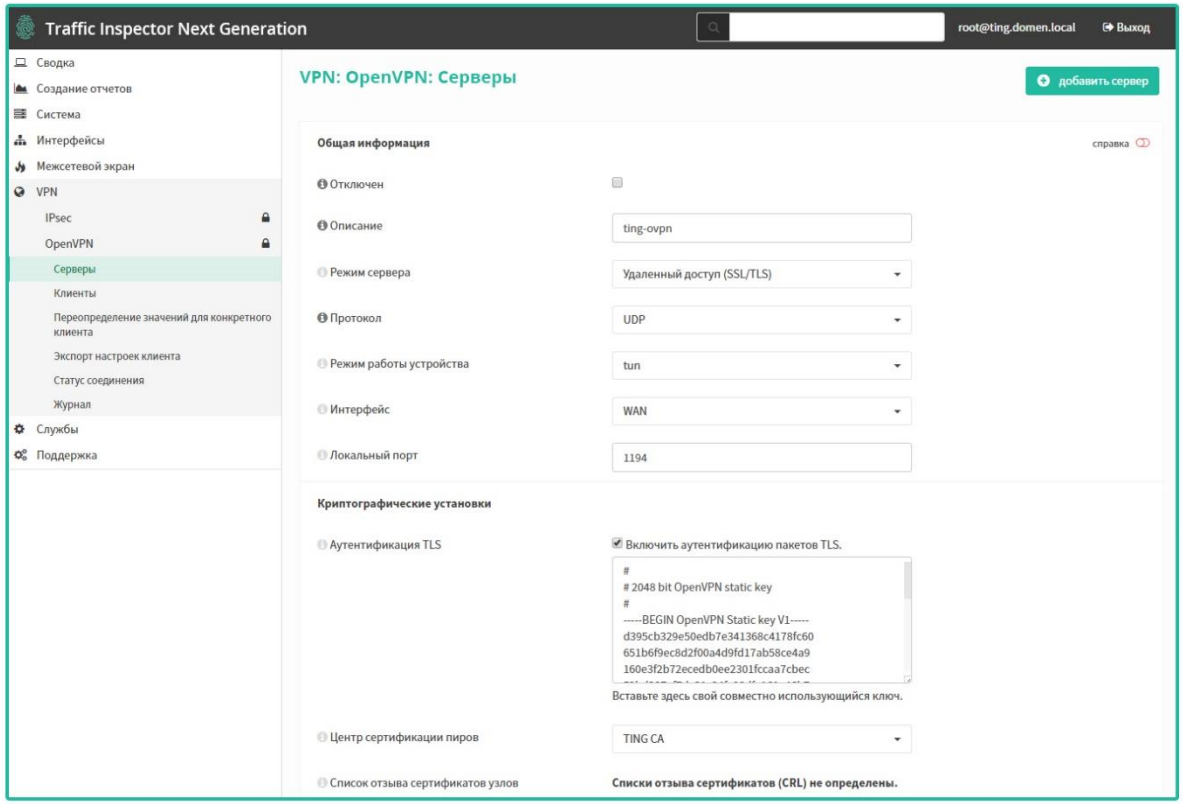
UserGate


UserGate
Главная консоль | Дашборд | Диагностика и мониторинг | Журналы и Отчеты | Временные пользователи | Помощь | Русский | Admin
UserGate UTM
Сеть
Пользователи и устройства
Политики сети
Межсетевой экран
NAT и маршрутизация
Балансировка нагрузки
Пропускная способность
Политики безопасности
Фильтрация контента
Веб-безопасность
Дешифрование
СОВ
Правила АСУ ТП
Сценарии
Защита почтового трафика
ICAP-правила
ICAP-серверы
Правила Reverse-прокси
Серверы Reverse-прокси
VPN
Серверные правила
Клиентские правила
Туннели VPN
Серверные профили
Оповещения
Правила оповещений
Профили оповещений
Библиотеки
Фильтрация контента
Добавить
Редактировать
Удалить
Переместить
Копировать
Включить
Отключить
Все
Обновить
Название Действие Категории Морфология URL Исходная ...
1 Example white list Разрешить Любая Любая Белый список ... Trusted
2 Example black list Запретить Любая Любая Черный список... Черный список... Черный список... Trusted
3 Example threats sites Запретить Threats Любая Любой Trusted
4 Example redirect to safesearch engines Запретить Любая Любая Поисковые сис... Trusted
5 Example parental control by categories Запретить Parental Control Threats Любая Любой Trusted
6 Example parental control by morphol... Запретить Recommended for morphology check... Нецензурная лекс... Наркотики Порнография Суицид ... Любой Trusted
7 Example AV check Запретить Recommended for virus check Любая Любой Trusted
8 Example Non-productive sites Предупр... Productivity Любая Любой Trusted
Наверх
Выше
Ниже
Вниз
Найти:

Traffic Inspector Next Generation

- Шлюзовый антивирус
- Контроль приложений
- Возможность балансировки нагрузки внутри сети

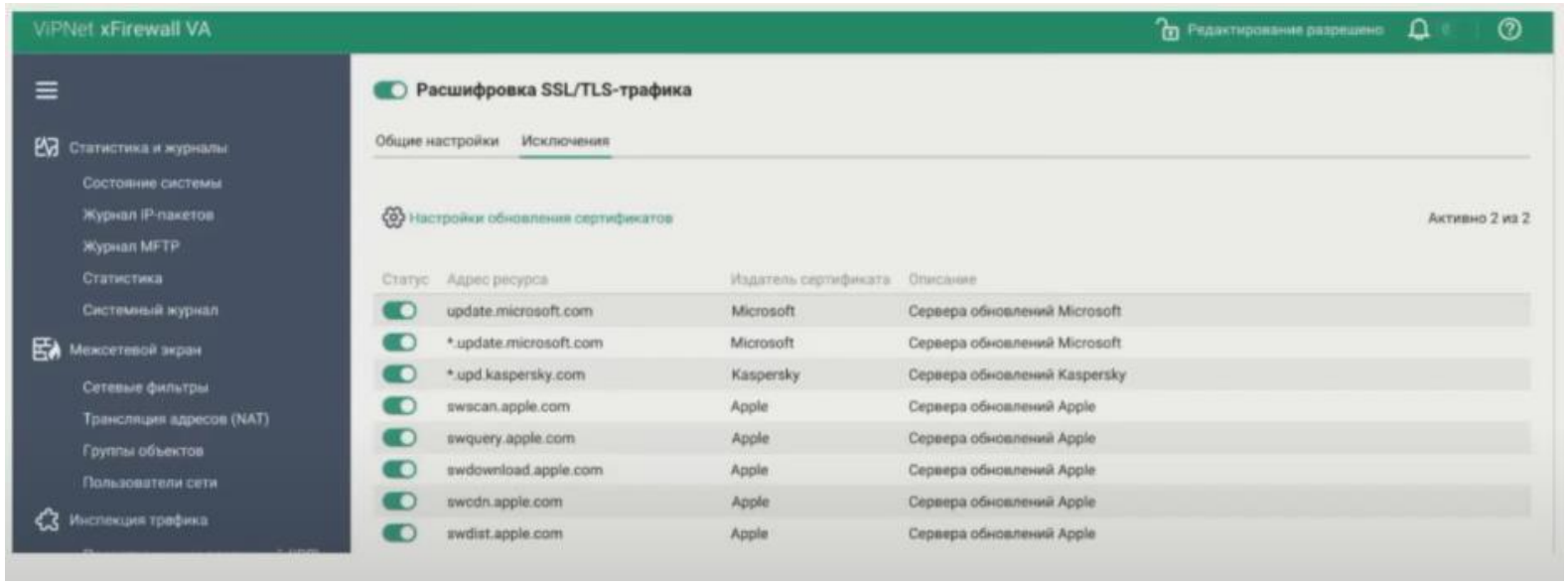
Traffic Inspector Next Generation



ViPNet xFirewall 5

- Контроль состояния сессий
- DPI
- Защита от спуфинга

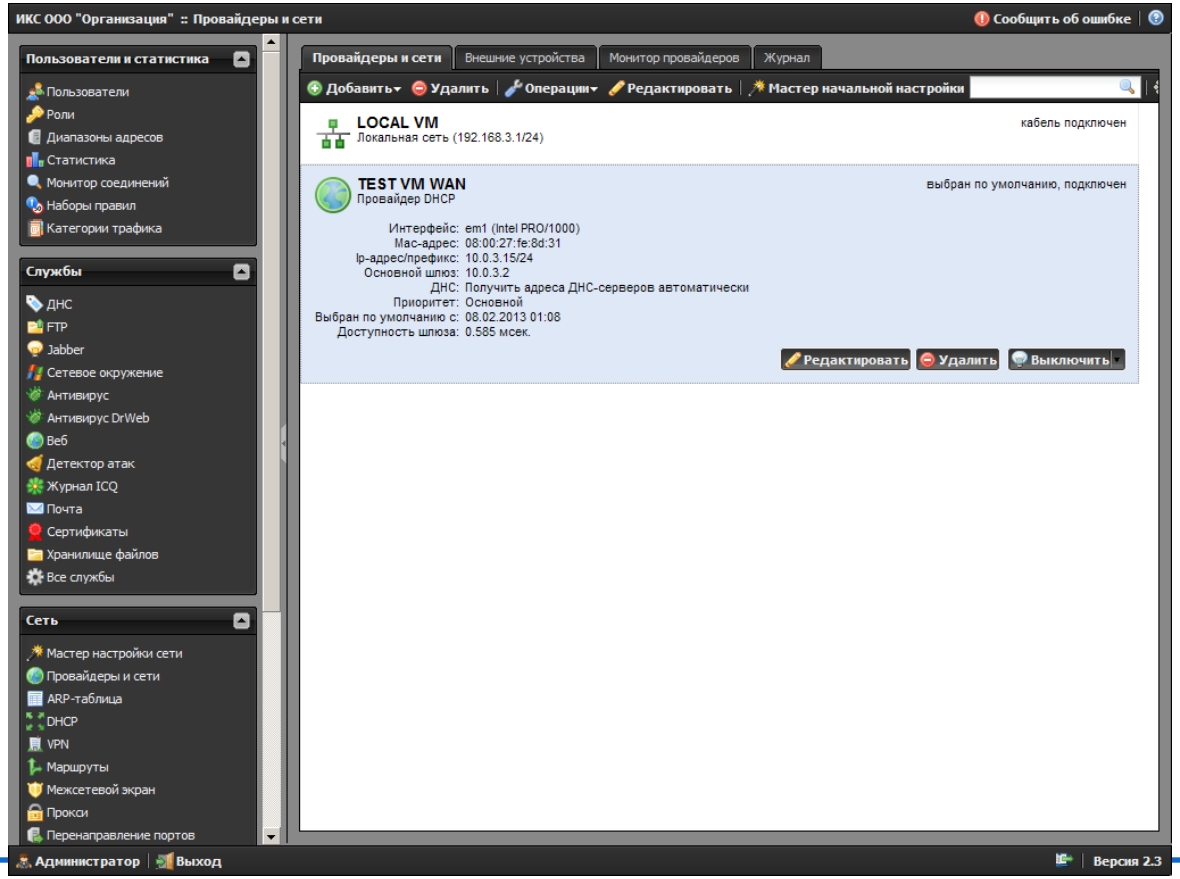
ViPNet xFirewall 5



Интернет контроль сервер

- Функции почтового сервера
- Функции сетевого и файлового хранилища
- Контроль доступа
- Учет трафика

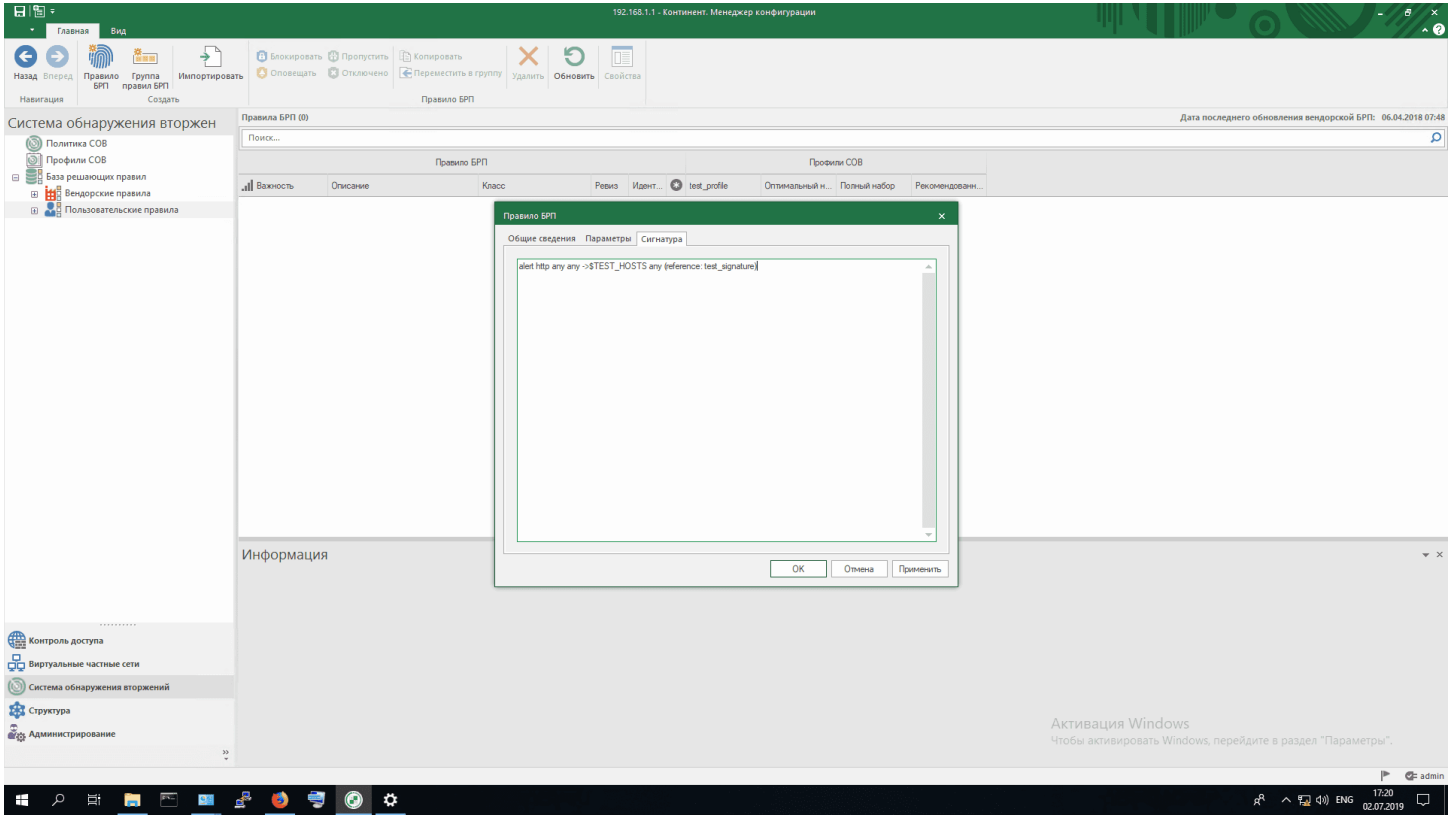
Интернет Контроль Сервер



Континент 4

- Поведенческий анализ трафика
- Контроль доступа на основе репутации адресов
- Контроль приложений

Континент 4

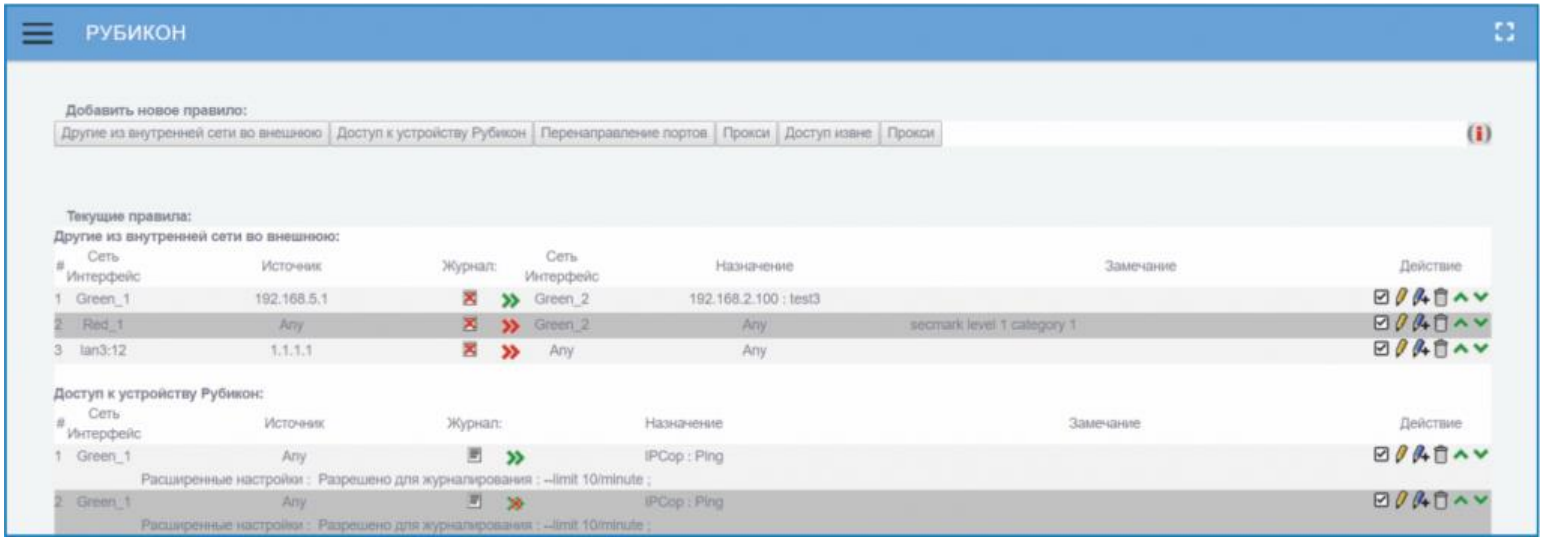

192.168.1.1 - Континент. Менеджер конфигурации
Главная
Вид
Назад
Вперед
Правило БРП
Группа правил БРП
Импортировать
Блокировать
Пропустить
Оповещать
Отключено
Копировать
Переместить в группу
Удалить
Обновить
Свойства
Навигация
Создать
Правило БРП
Система обнаружения вторжен
Политика СОВ
Профили СОВ
База решающих правил
Вендорские правила
Пользовательские правила
Правила БРП (0)
Дата последнего обновления вендорской БРП: 06.04.2018 07:48
Поиск...
Правило БРП
Профили СОВ
Важность
Описание
Класс
Ревиз
Идент...
test_profile
Оптимальный н...
Полный набор
Рекомендованн...
Правило БРП
Общие сведения
Параметры
Сигнатура
alert http any any ->$TEST_HOSTS any (reference: test_signature;)
OK
Отмена
Применить
Информация
Контроль доступа
Виртуальные частные сети
Система обнаружения вторжений
Структура
Администрирование
Активация Windows
Чтобы активировать Windows, перейдите в раздел "Параметры".
admin
ENG
17:20
02.07.2019

Рубикон

- Интеграция с SIEM (?)
- Статическая и динамическая маршрутизация
- Резервирование на уровне устройств, портов, каналов

Рубикон

Правила фильтрации



Traffic Inspector Next Generation

- Фильтрует трафик на разных уровнях

Межсетевой экран следующего поколения (NGFW)

- Next-generation firewall (NGFW) – файрвол следующего поколения. Его ключевая особенность в том, что он может производить фильтрацию не только на уровне протоколов и портов, но и на уровне приложений и их функций. Это позволяет успешнее отражать атаки и блокировать вредоносную активность.
- Также, в отличие от межсетевого экрана типа Unified threat management, у NGFW есть более детальная настройка политик безопасности и решения для крупного бизнеса.

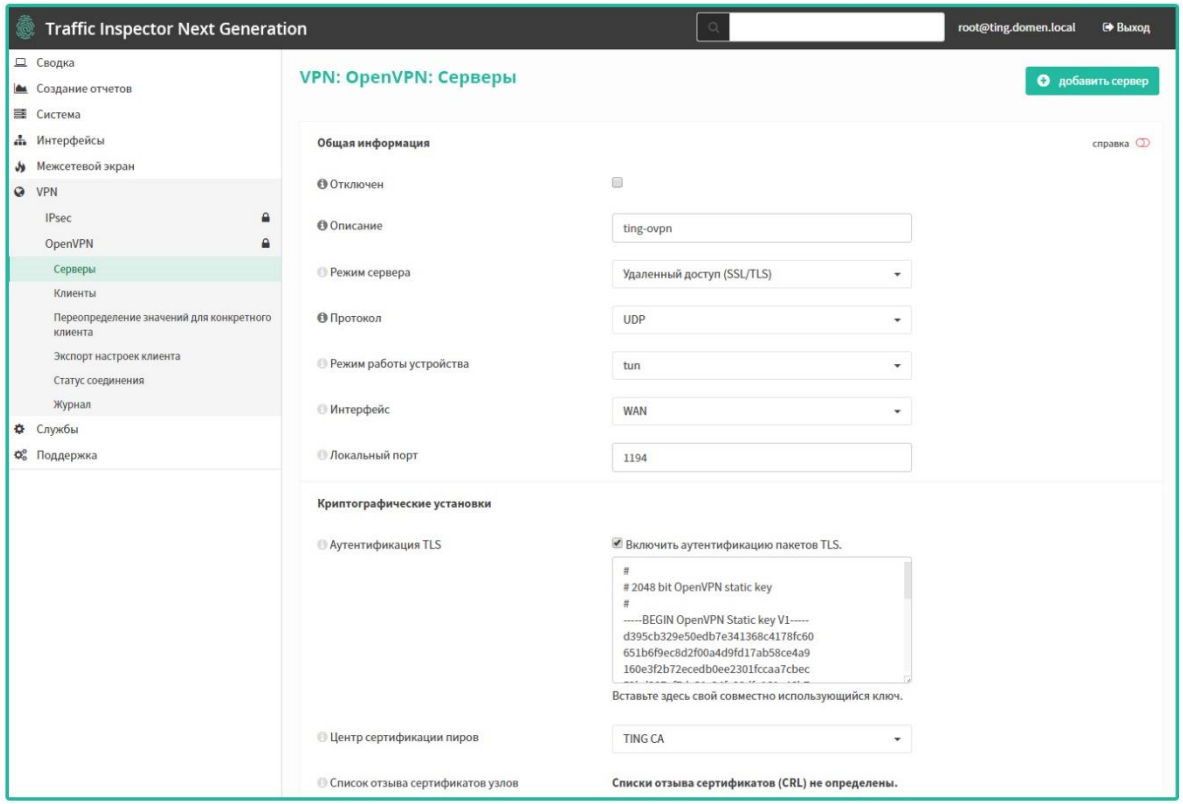
Основные функции Next-generation firewall

- **Deep Packet Inspection** (DPI) – технология, выполняющая детальный анализ пакетов. В отличие от правил классического межсетевого экрана данная технология позволяет выполнять анализ пакета на верхних уровнях модели OSI. Помимо этого, DPI выполняет поведенческий анализ трафика, что позволяет распознавать приложения, которые не используют заранее известные заголовки и структуры данных.
- **Intrusion Detection System/ Intrusion Prevention System** (IDS/IPS) — система обнаружения и предотвращения вторжений. Межсетевой экран блокирует и фильтрует трафик, в то время как IPS/IDS обнаруживает вторжение и предупреждает системного администратора или предотвращает атаку в соответствии с конфигурацией.
- **Антивирус**. Обеспечивает защиту от вирусов и шпионского ПО в реальном времени, определяет и нейтрализует вредонос на различных платформах

- **Фильтрация по URL, или веб-фильтр**, — возможность блокировки доступа к сайтам или другим веб-приложениям по ключевому слову в адресе.
- **Инспектирование SSL**. Позволяет межсетевому экрану нового поколения устанавливать SSL-сессию с клиентом и сервером. Благодаря этому существует возможность просматривать шифрованный трафик и применять к нему политики безопасности.
- **Антиспам** — функция, которая позволяет защитить корпоративных пользователей от фишинговых и нежелательных писем
- **Application Control**. Используется для ограничения доступа к приложениям, их функциям или к целым категориям приложений. Все это задействует функции отслеживания состояния приложений, запущенных пользователем, в режиме реального времени.

- **Web Application Firewall** — совокупность правил и политик, направленных на предотвращение атак на веб-приложения
- **Аутентификация пользователей** — возможность настраивать индивидуальные правила под каждого пользователя или группу.
- **Sandboxing**. Метод, при котором файл автоматически помещается в изолированную среду для тестирования, или так называемую песочницу. В ней можно инициализировать выполнение подозрительной программы или переход по URL, который злоумышленник может прикрепить к письму. Песочница создает безопасное место для установки и выполнения программы, не подвергая опасности остальную часть системы.

Traffic Inspector Next Generation

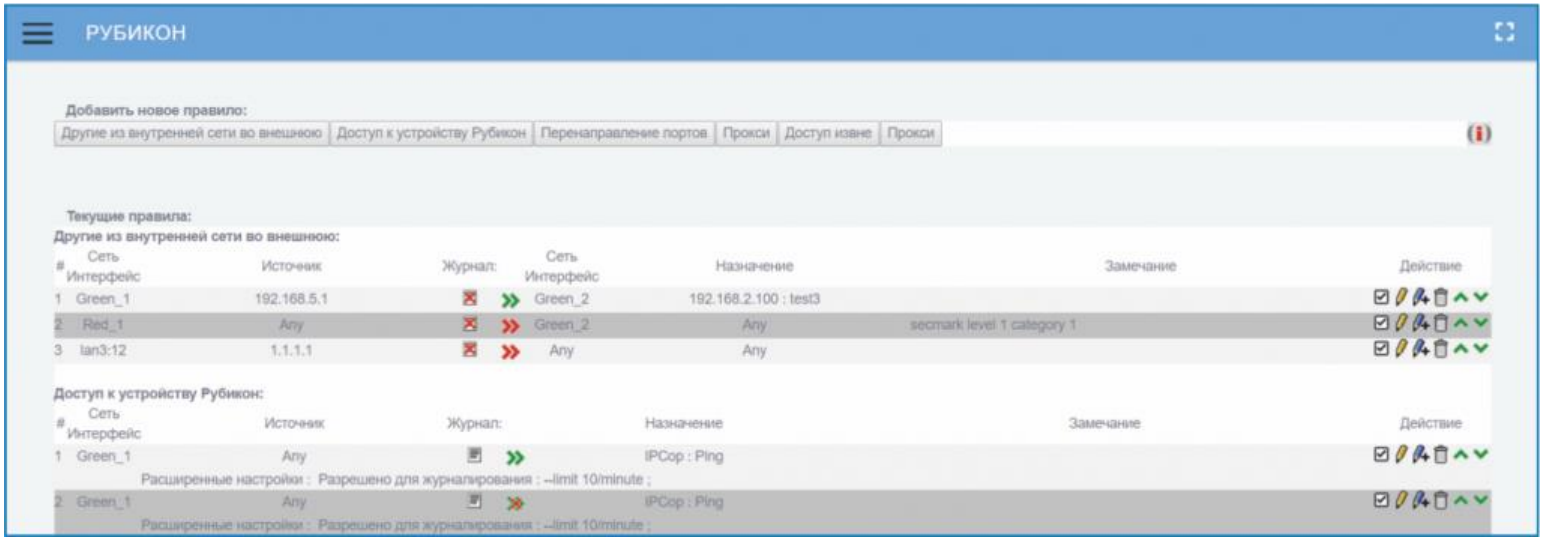


Рубикон

РУБИКОН

Рубикон

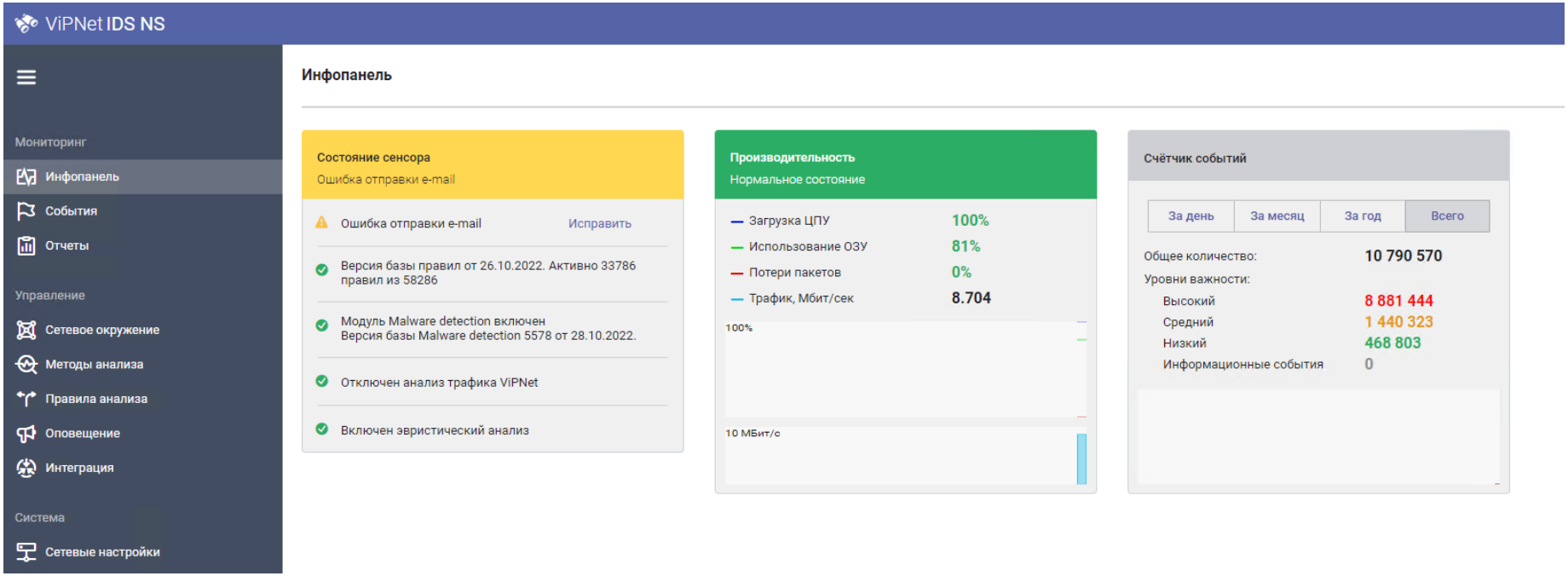
Правила фильтрации



ViPNet IDS NS

- Непрерывный мониторинг
- Рекомендации по устранению
- Предотвращение повторения угроз (?)
- Отчеты

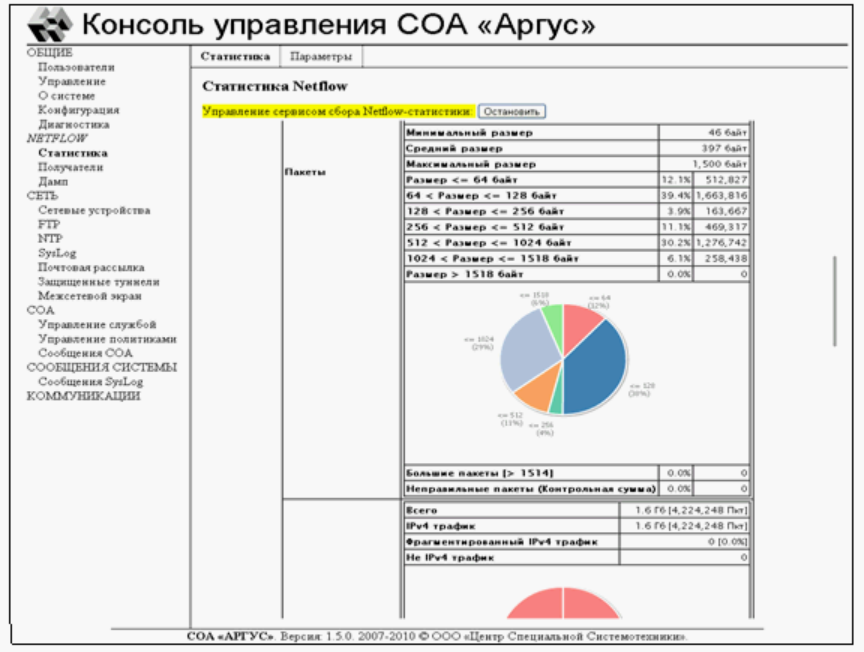
ViPNet IDS NS



Аргус

- Выявление вторжений и подозрительных воздействий
- Расследование инцидентов

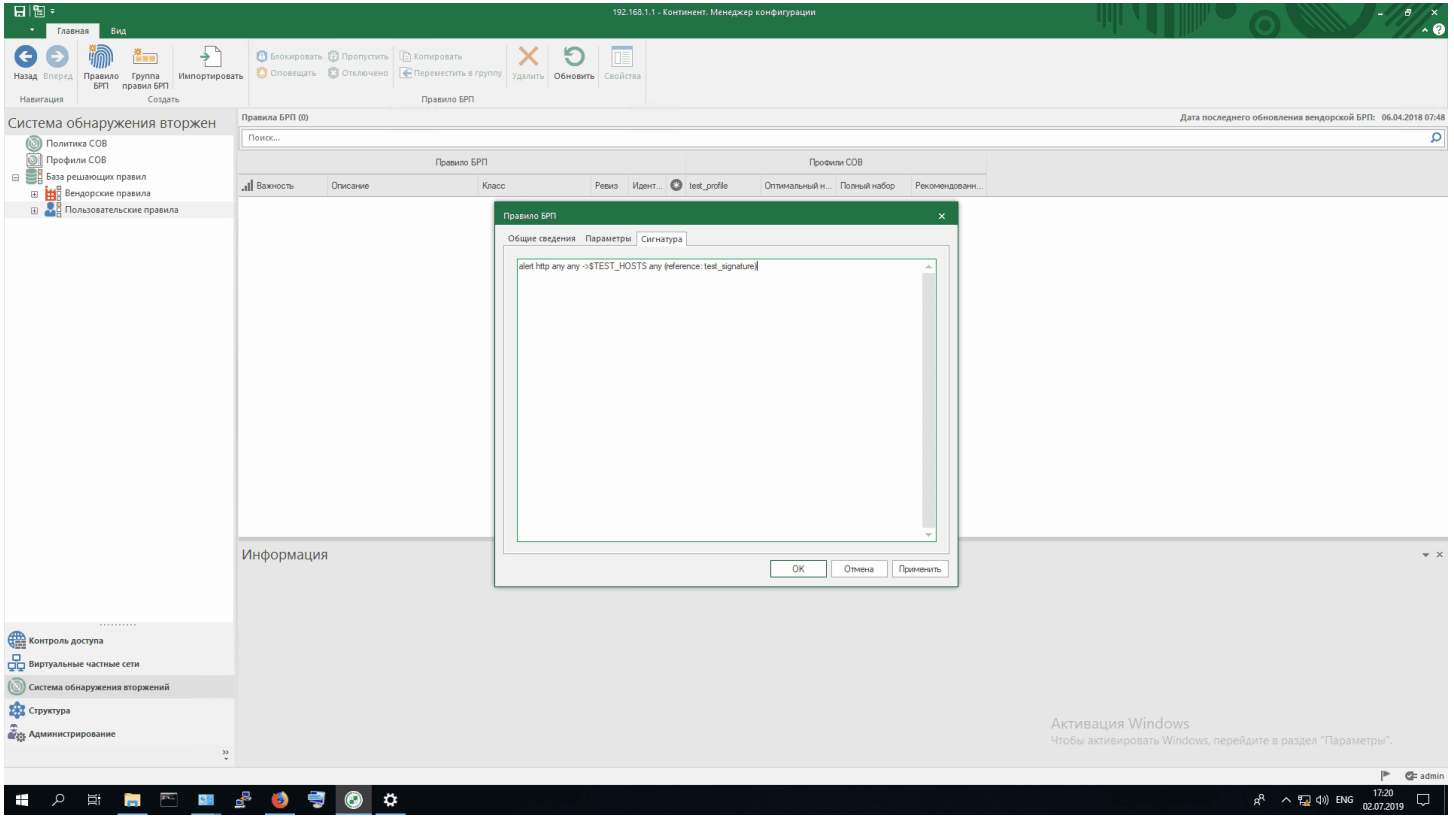
Аргус


Консоль управления СОА «Аргус»
ОБЩИЕ
Пользователи
Управление
О системе
Конфигурация
Диагностика
NETFLOW
Статистика
Получатели
Дамп
СЕТЬ
Сетевые устройства
FTP
NTP
SysLog
Почтовая рассылка
Защищенные туннели
Межсетевой экран
СОА
Управление службой
Управление политиками
Сообщения СОА
СООБЩЕНИЯ СИСТЕМЫ
Сообщения SysLog
КОММУНИКАЦИИ
Статистика
Параметры
Статистика Netflow
Управление сервисом сбора Netflow-статистики:
Остановить
Пакеты
Минимальный размер 46 байт
Средний размер 397 байт
Максимальный размер 1,500 байт
Размер <= 64 байт 12.1% 512,827
64 < Размер <= 128 байт 39.4% 1,663,816
128 < Размер <= 256 байт 3.9% 163,667
256 < Размер <= 512 байт 11.1% 469,317
512 < Размер <= 1024 байт 30.2% 1,276,742
1024 < Размер <= 1518 байт 6.1% 258,438
Размер > 1518 байт 0.0% 0
Большие пакеты [> 1514] 0.0% 0
Неправильные пакеты (Контрольная сумма) 0.0% 0
Всего 1.6 Гб [4,224,248 Пкт]
IPv4 трафик 1.6 Гб [4,224,248 Пкт]
Фрагментированный IPv4 трафик 0 [0.0%]
Не IPv4 трафик 0
СОА «АРГУС» Версия 1.5.0. 2007-2010 © ООО «Центр Специальной Системотехники».

СОВ Континент

- Отслеживание и управление событиями
- Онлайн-режим предупреждения атак
- DPI

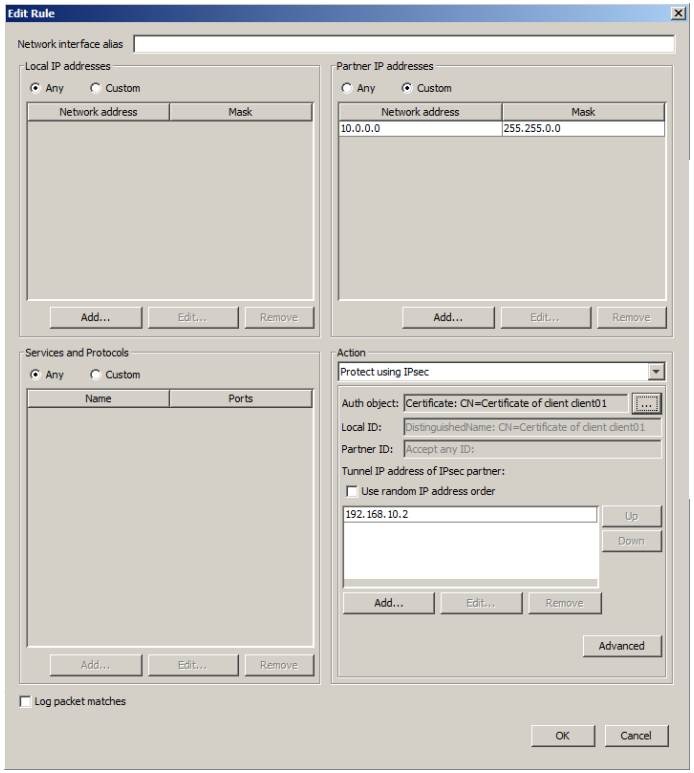
СОВ Континент



С-Терра СОВ

- Анализ сетевого трафика
- Механизмы сетевого анализа

C-Teppa COB


Edit Rule
Network interface alias
Local IP addresses
Any
Custom
Network address
Mask
Add...
Edit...
Remove
Partner IP addresses
Any
Custom
Network address
Mask
10.0.0.0
255.255.0.0
Add...
Edit...
Remove
Services and Protocols
Any
Custom
Name
Ports
Add...
Edit...
Remove
Action
Protect using IPsec
Auth object:
Certificate: CN=Certificate of client client01
Local ID:
DistinguishedName: CN=Certificate of client client01
Partner ID:
Accept any ID:
Tunnel IP address of IPsec partner:
Use random IP address order
192.168.10.2
Up
Down
Add...
Edit...
Remove
Advanced
Log packet matches
OK
Cancel


s•terra

Использование прокси в качестве межсетевого экрана

- Прокси-сервер контролирует трафик на последнем уровне стека TCP\IP, поэтому иногда его называют шлюзом приложений. Принцип работы заключается в фильтрации данных на основании полей заголовков, содержимого поля полезной нагрузки и их размеров (помимо этого, задаются дополнительные параметры фильтрации).
- Прокси-серверы осуществляют фильтрацию одного или нескольких протоколов. Например, наиболее распространенным прокси-сервером является веб-прокси, предназначенный для обработки веб-трафика.

Такие серверы используются для следующих целей:
•обеспечение безопасности — например, для защиты вашего веб-сайта или пользователей от посещения сторонних сайтов,
•повышение производительности сети,
•ускорение доступа к некоторым ресурсам в интернете и др.
Поскольку прокси-серверы предназначены для определенных протоколов/портов, они, как правило, имеют более глубокие и сложные средства управления, чем общие правила безопасности межсетевого экрана.
Помимо веб-прокси, существуют такие прокси-серверы, как DNS, FTP, telnet, SSH, SSL, и другие протоколы.

СИСТЕМЫ АНАЛИЗА ТРАФИКА, ОБНАРУЖЕНИЯ И ПРЕДОТВРАЩЕНИЯ АТАК

Системы анализа трафика NTA

Системы мониторинга и анализа сетевого трафика (Network Traffic Analysis, NTA) выявляют угрозы информационной безопасности, исследуя события на уровне сети. Они позволяют обнаружить присутствие злоумышленников на ранней стадии атаки, оперативно локализовать угрозы и контролировать соблюдение регламентов ИБ.

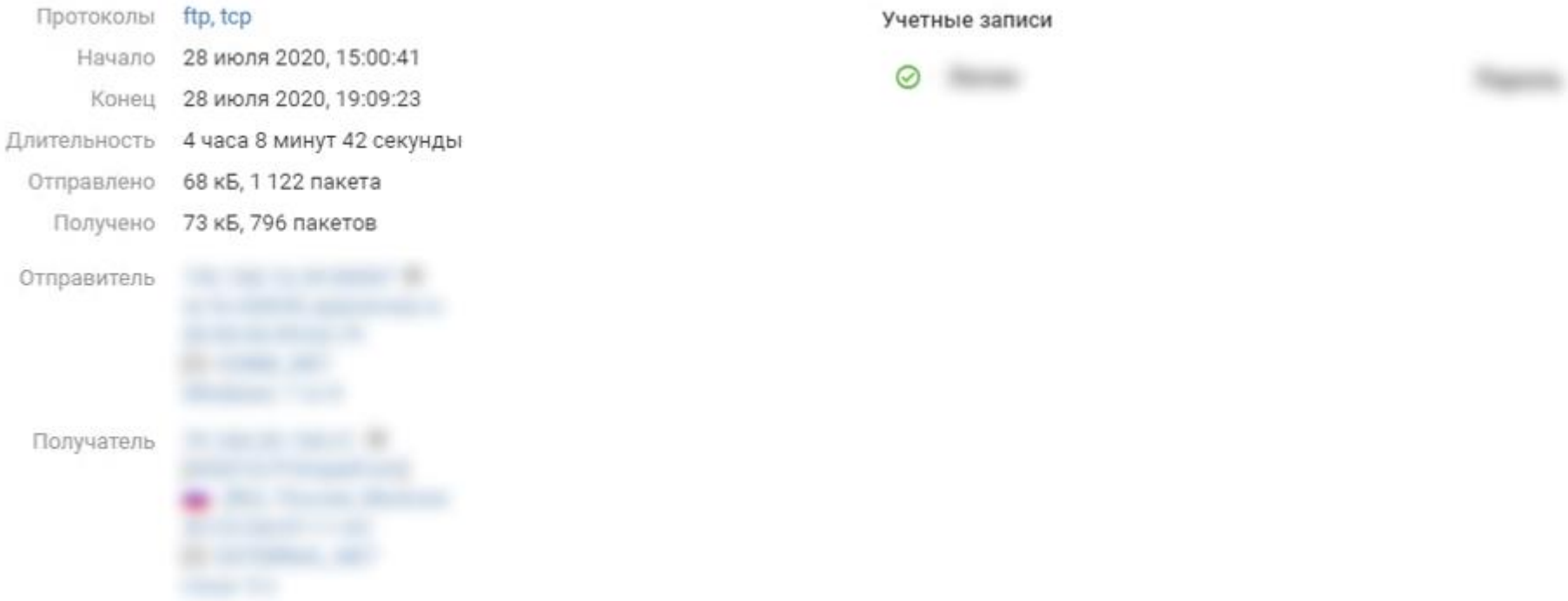
В инфраструктуру каждой второй компании можно проникнуть всего за один шаг. При этом, когда злоумышленники попадают во внутреннюю сеть, все их действия становятся незаметными для периметровых средств защиты. Получив такой доступ к системе, можно очень долго избегать обнаружения и оставаться невидимкой. Рекорд, зафиксированный специалистами PT Expert Security Center, составил более 8 лет.

Чтобы не дать развить атаку внутри инфраструктуры, важно отслеживать безопасность сети. В этом помогает сигнатурный анализ трафика с помощью NTA-систем.

Три ключевых отличия NTA от других решений, работающих с трафиком:
1.Анализ трафика и на периметре, и в инфраструктуре. Другие системы, работающие с трафиком (IDS/IPS, межсетевые экраны), в отличии от NTA, стоят только на периметре, не внутри. Поэтому, когда злоумышленники проникают в сеть, их действия становятся незаметными.
2.Выявление атак с помощью комбинации способов. Машинное обучение, поведенческие факторы, правила детектирования, индикаторы компрометации, ретроспективный анализ позволяют обнаруживать атаки и на ранних стадиях, и когда злоумышленник уже проник в инфраструктуру.
3.Применение NTA помогает в обнаружении и расследовании инцидентов и в threat hunting, проактивном поиске сетевых угроз, которые не обнаруживаются традиционными средствами анализа безопасности siem-систем. NTA-системы хранят информацию о сетевых взаимодействиях, а некоторые из них - еще и запись сырого трафика. Такие данные становятся полезными источниками знаний при анализе и раскрутке цепочки сетевой атаки и ее локализации, а также при проверке гипотез в рамках threat hunting.

Пример №1

Подключение к файловым серверам с раскрытием учетных данных:



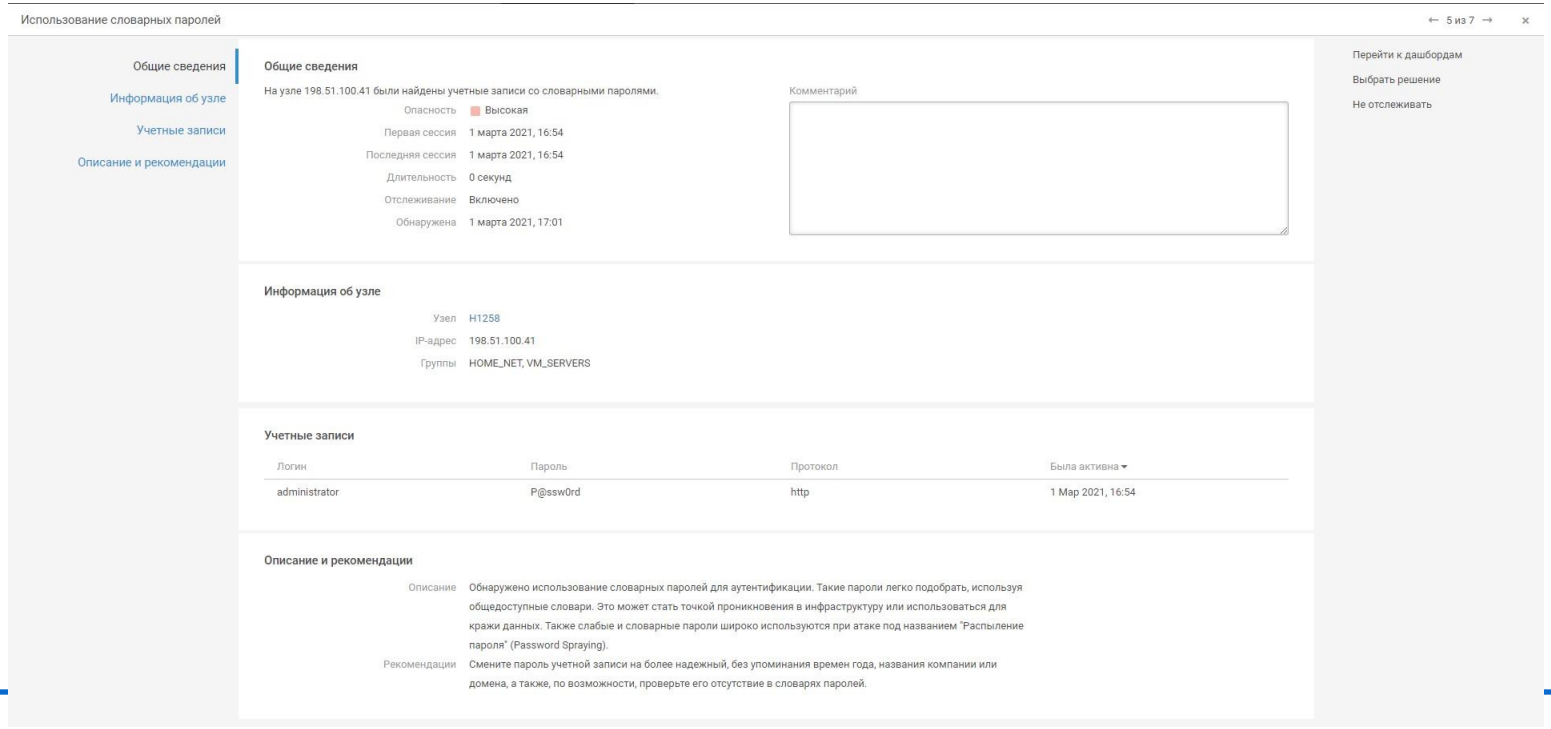
С помощью фильтра в PT NAD можно настроить виджет, где будут отображаться все открытые пароли:

Пары "логин — пароль" по числу сессий

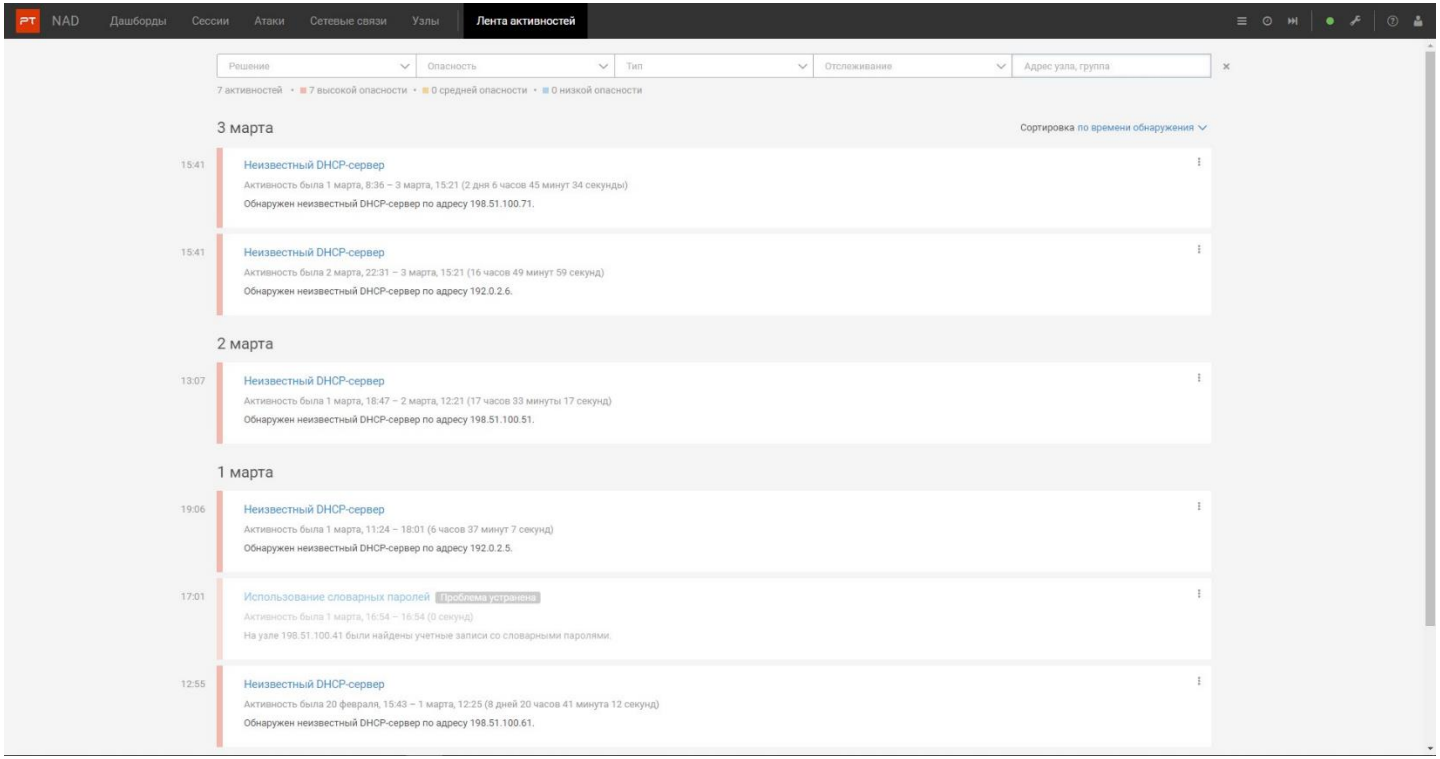
Логин	Пароль	Количество се...
admin	Password	14642
admin	admin	514
Bob	alice	393
Alice	bob	204
proxy	secret123!	129
tg	123qwerty	102
proxyuser	superpassword	74
tlauser	KWidiochsh8^*6dewif	64

Пример №2

PT NAD позволяет своевременно реагировать и выявлять такие инциденты, как нарушение комплаенса со стороны пользователей. Рассмотрим на примере.
В ленте активностей появилось уведомление об использовании словарных паролей. С помощью информации об узле оператор PT NAD находит пользователя и обращается к нему с требованием сменить пароль на более надежный.

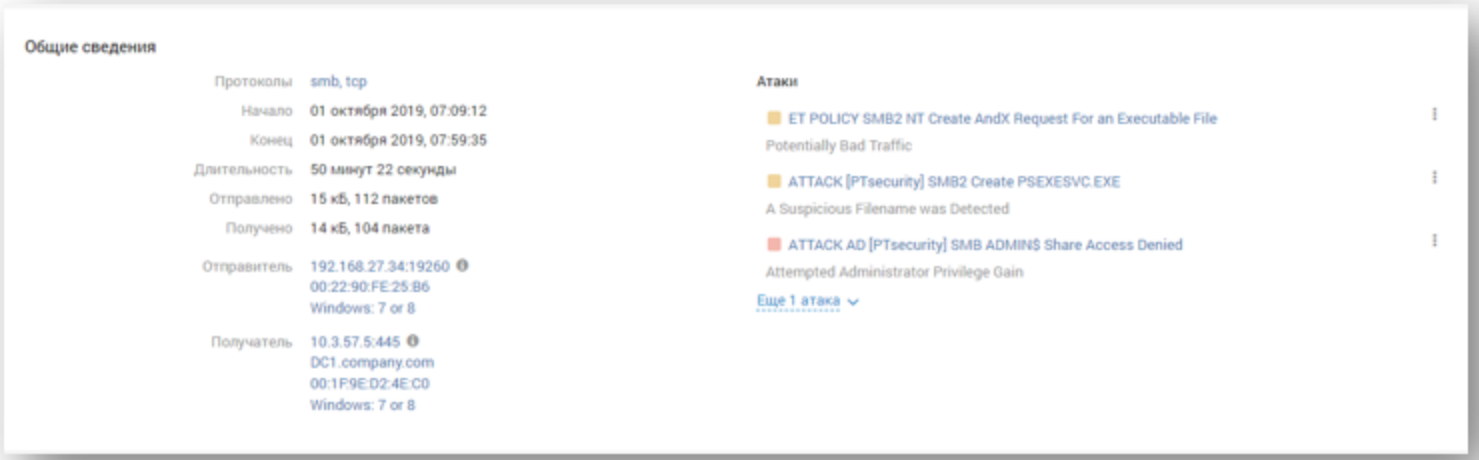


После этого оператор указывает в карточке активности, что проблема была решена.

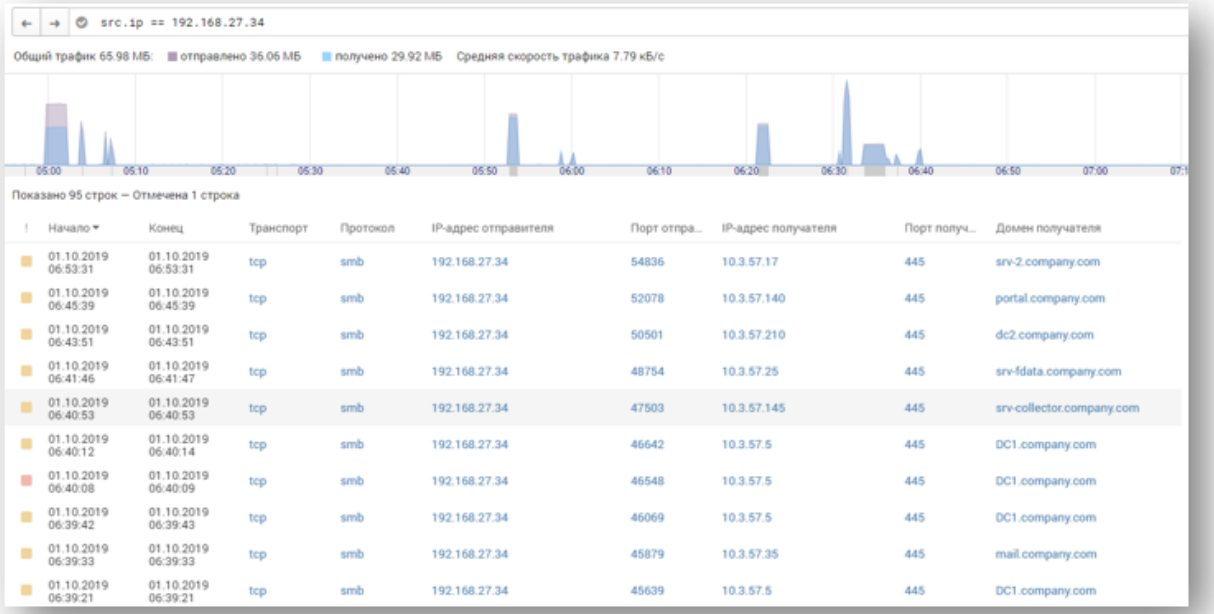


Пример 3

Рассмотрим пример расследования атаки. PT NAD уведомил о неуспешной попытке авторизации в контроллере домена с учетной записи, не имеющей достаточного объема прав.



После проверки сетевой активности узла выявлено, что ранее с него уже было предпринято несколько попыток подключений на другие хосты во внерабочее время.



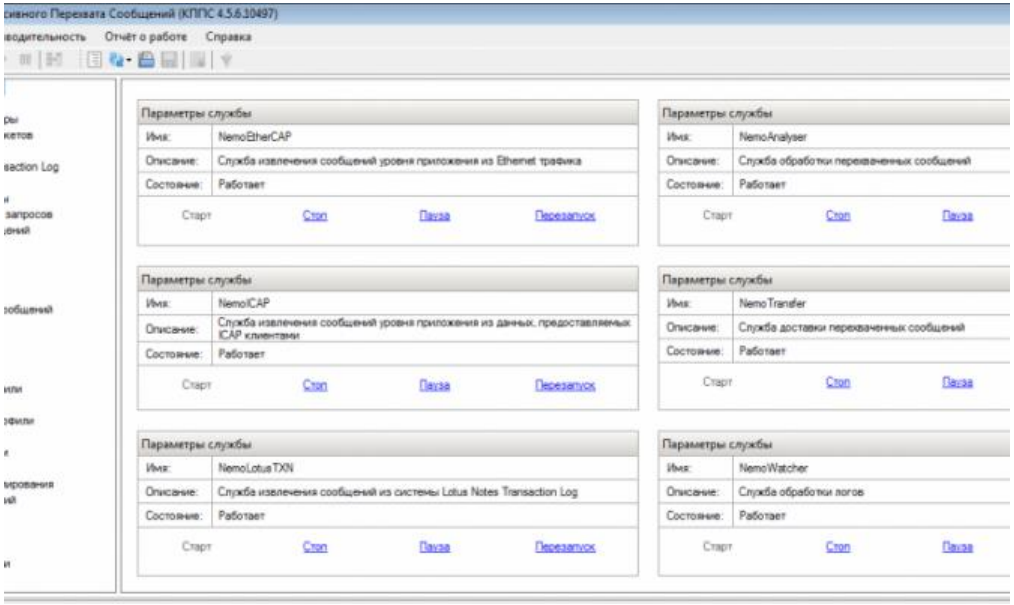
!	Начало	Конец	Транспорт	Протокол	IP-адрес отправителя	Порт отпра...	IP-адрес получателя	Порт получ...	Домен получателя
	01.10.2019 06:53:31	01.10.2019 06:53:31	tcp	smb	192.168.27.34	54836	10.3.57.17	445	srv-2.company.com
	01.10.2019 06:45:39	01.10.2019 06:45:39	tcp	smb	192.168.27.34	52078	10.3.57.140	445	portal.company.com
	01.10.2019 06:43:51	01.10.2019 06:43:51	tcp	smb	192.168.27.34	50501	10.3.57.210	445	dc2.company.com
	01.10.2019 06:41:46	01.10.2019 06:41:47	tcp	smb	192.168.27.34	48754	10.3.57.25	445	srv-fdata.company.com
	01.10.2019 06:40:53	01.10.2019 06:40:53	tcp	smb	192.168.27.34	47503	10.3.57.145	445	srv-collector.company.com
	01.10.2019 06:40:12	01.10.2019 06:40:14	tcp	smb	192.168.27.34	46642	10.3.57.5	445	DC1.company.com
	01.10.2019 06:40:08	01.10.2019 06:40:09	tcp	smb	192.168.27.34	46548	10.3.57.5	445	DC1.company.com
	01.10.2019 06:39:42	01.10.2019 06:39:43	tcp	smb	192.168.27.34	46069	10.3.57.5	445	DC1.company.com
	01.10.2019 06:39:33	01.10.2019 06:39:33	tcp	smb	192.168.27.34	45879	10.3.57.35	445	mail.company.com
	01.10.2019 06:39:21	01.10.2019 06:39:21	tcp	smb	192.168.27.34	45639	10.3.57.5	445	DC1.company.com

С помощью ИТ-службы безопасности утечка была выявлена и заблокирована. Началось детальное расследование с командой PT ESC.

EtherSensor

- DPI в реальном времени
- Содержимое сообщений
- Файлы
- Действия в сервисах
- Метаданные

Ether Sensor

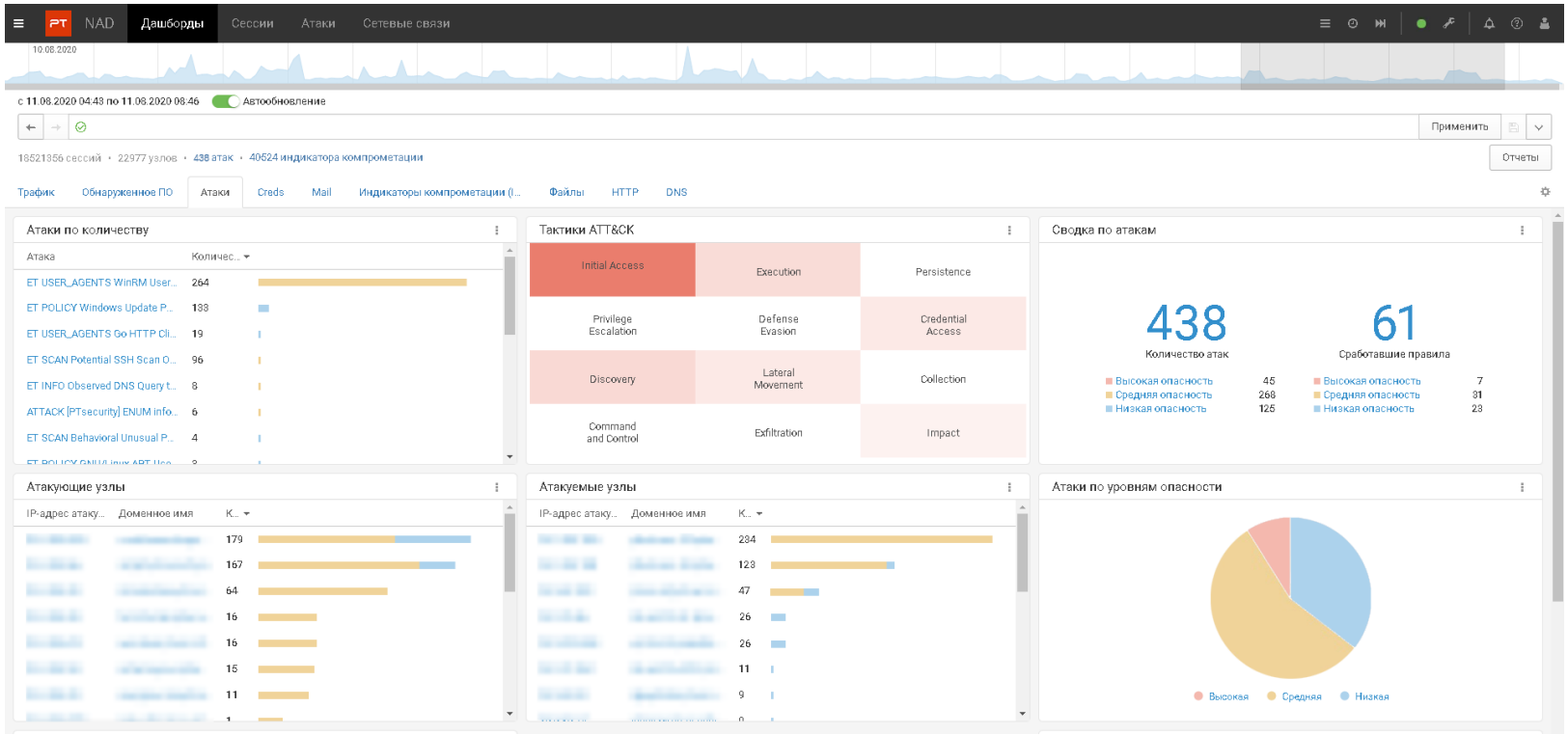


PT Network Attack Discovery

- DPI в реальном времени
- Автоматическое моделирование по матрице MITRE
- Пока сыроват

positive technologies

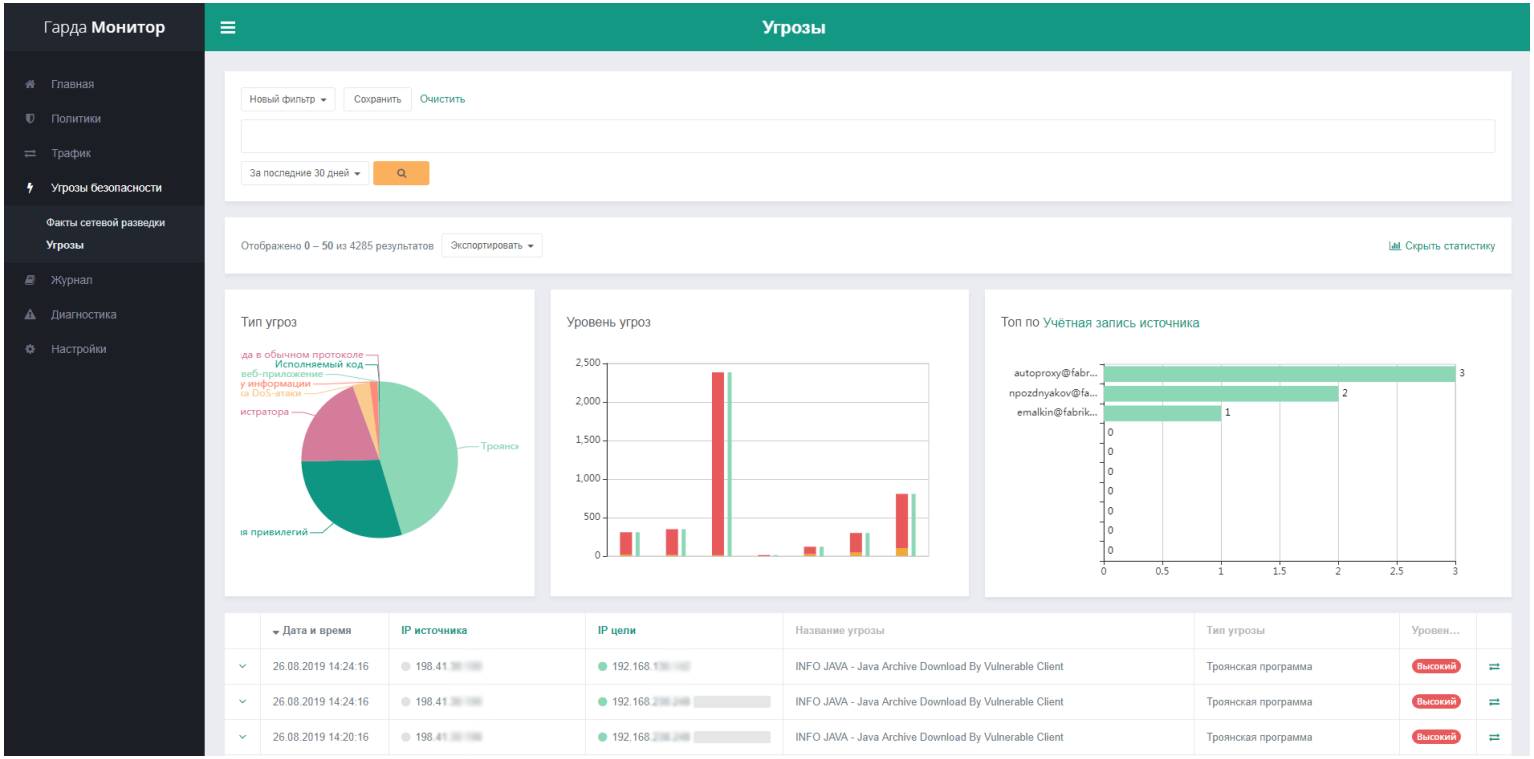
PT Network Attack Discovery



Гарда Монитор

- DPI в реальном времени
- Запись трафика, индексация и поиск

Гарда Монитор



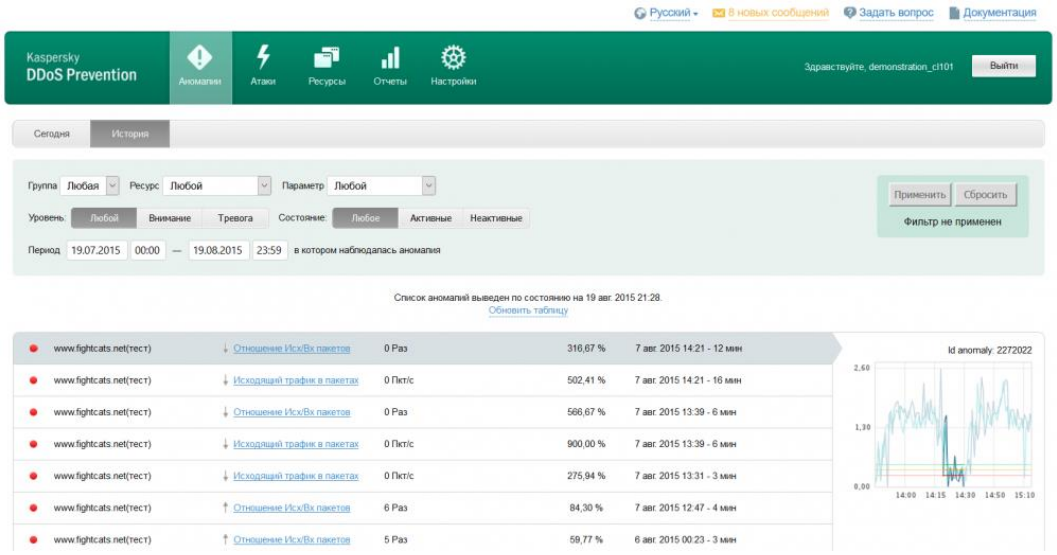
ЗАЩИТА ОТ DDOS-АТАК

DDoS-Guard

- Только облако
- Защита на основе ИИ
- Использование Reverse Proxy
- DNS-хостинг

Kaspersky DDoS Protection

- Облако/гибрид
- Центры очистки для блокировки паразитного трафик
- Классификация посетителей
- Поведенческий анализ для проверки без расшифровки трафика



Облачная защита от DDoS-атак (МегаФон)

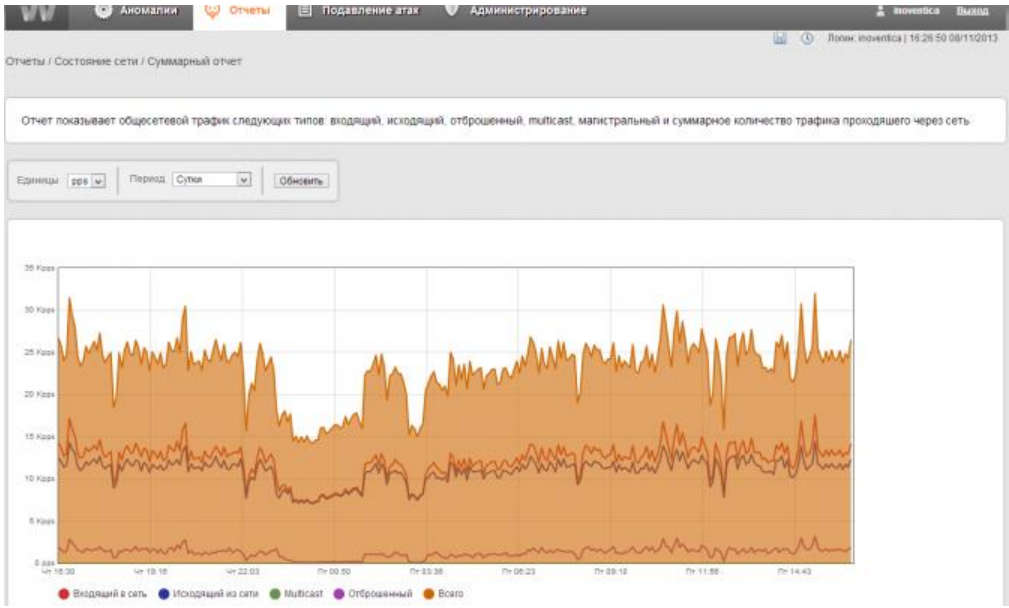
- Только облако
- Выделенная служба мониторинга и реагирования
- Защита трафика без дешифрации
- Защита на L3, L4, L7

Периметр

- Анализ «сырого» трафика
- Обнаружение и подавление атак и аномалий
- Мониторинг сетевого трафика

invGUARD

- Анализ и очистка без передачи трафика вовне
- Эвристические алгоритмы
- Не влияет на скорость передачи



Митигатор

- ПАК
- Интеграция с системами защиты и мониторинга
- Поддержка BGP FlowSpec

ШЛЮЗЫ БЕЗОПАСНОСТИ

Шлюзы сетевой безопасности (Secure Web Gateway, SWG) представляют собой программно-аппаратные комплексы, которые обеспечивают защищённый доступ к интернету и возможность безопасного использования веб-приложений. Они помогают защищаться от вредоносных действий со стороны инсайдеров, а также нейтрализуют эксплуатацию уязвимостей на стороне внутренней сети предприятия.

Шлюзы SWG развёртываются на границе, разделяющей внешнюю и внутреннюю сети компании. Такой вариант позволяет защитить все ресурсы предприятия ото внешнего вредоносного влияния. Даже если на пользовательских компьютерах во внутренней сети нет антивируса, установленный шлюз помогает заблокировать соединение со вредоносным ресурсом при попытке передать код вируса.

Благодаря шлюзам SWG обеспечивается защита от вредоносного кода, размещаемого внутри веб-трафика. Шлюзы осуществляют фильтрацию сайтов с учётом их категорий и репутации, выполняют проверку приложений, помогают блокировать ботнет-трафик и обнаруживать утечки данных.

Универсальный шлюз безопасности (UTM) – это единая система информационной безопасности (сетевое аппаратное устройство, виртуальное устройство или "облачная" служба, которая защищает предприятия от угроз безопасности, объединяя и интегрируя множество служб и функций безопасности.

Устройства UTM часто упаковываются как устройства сетевой безопасности, которые могут помочь защитить сети от комбинированных угроз безопасности, включая вредоносные программы и атаки, которые одновременно направлены на отдельные части сети.

"Облачные" службы UTM и виртуальные сетевые устройства становятся все более популярными для обеспечения сетевой безопасности, особенно для малого и среднего бизнеса. И те, и другие избавляют от необходимости в локальных устройствах сетевой безопасности, обеспечивая при этом централизованный контроль и простоту использования для глубокого построения системы защиты сети.

Универсальные шлюзы безопасности (UTM) предлагают несколько уровней сетевой безопасности, включая брандмауэры, системы обнаружения/предотвращения вторжений, антивирусы, виртуальные частные сети (VPN), фильтрацию спама и URL-адресов для веб-содержимого.

Возможности UTM

• **Межсетевое экранирование.** Брандмауэры ограничивают создание сетевых соединений между узлами внутри организации и за ее пределами с целью уменьшения или устранения воздействия внешних узлов, сетей или протоколов, которые, как известно, являются векторами сетевых угроз;
• **Антивирус.** Обеспечивают централизованную антивирусную проверку трафика пользователей на уровне шлюза;
• **Антиспам.** Службы защиты от спама блокируют или помечают входящие почтовые атаки, сканируя входящий и исходящий почтовый трафик. Фильтрация спама позволяет предприятиям использовать сторонние серверные блокировочные списки спама или создавать собственные локальные белые и черные списки для фильтрации сообщений электронной почты;
• **Авторизация пользователей.** Аутентификация, включая двухфакторную, может производится с помощью локальной базы пользователей, службы каталогов LDAP, Kerberos, Radius-сервера;
• **VPN.** VPN обеспечивает защищенный туннель, через который может проходить сетевая активность. VPN можно настроить для туннелирования всего трафика от мобильных узлов до устройств UTM, позволяя применять все проверки безопасности сети UTM к мобильному трафику и снижая количество инцидентов безопасности, связанных с этими устройствами;

Обнаружение и предотвращение вторжений (IDS/IPS). Выявляют и предотвращают атаки, обнаруживая, когда злоумышленник пытается получить доступ к сети, и предотвращая эти типы атак. Наиболее эффективные UTM-устройства и службы решают проблемы этого типа угроз безопасности с помощью комбинации методов, включая обнаружение атак на основе сигнатур вредоносных программ, аномалий или обнаружение на основе репутации, чтобы остановить как известные, так и неизвестные атаки;

• **Контроль приложений. Ограничивают** или блокируют трафик определенных интернет-приложений. Глубокая инспекция пакетов позволяет просто и эффективно блокировать приложения, например Skype или BitTorrent;

• **Контентная фильтрация.** Возможности веб-фильтрации для контента и фильтрации URL-адресов охватывают ряд техник, которые определяют, должен ли веб-запрос, связанный с веб-сайтом или URL-адресом, быть разрешен или нет. Некоторые UTM используют аналитические методы, которые способны сканировать веб-сайты на наличие нарушений безопасности, указывающих на то, что веб-сайт может представлять собой угрозу безопасности.

UTM особенно полезны в организациях, которые имеют много филиалов или торговых точек, которые традиционно использовали выделенную WAN, но все чаще используют общедоступные интернет-подключения к головному офису/центру обработки данных. Использование UTM в этих случаях дает бизнесу больше информации и лучший контроль над безопасностью этих филиалов или торговых точек.

Предприятия могут выбрать один или несколько методов развертывания UTM на соответствующих платформах, но они также могут найти наиболее подходящий вариант для выбора комбинации платформ. Некоторые из вариантов включают установку программного обеспечения UTM на серверах компании в центре обработки данных; использование программных продуктов UTM на "облачных" серверах; использование традиционных аппаратных устройств UTM, которые поставляются с предварительно интегрированным аппаратным и программным обеспечением или использование виртуальных устройств, которые представляют собой интегрированные программные комплекты, которые можно развернуть в виртуальных средах.

Kaspersky Security для интернет-шлюзов

- Программный продукт
- Персональный МЭ
- Система мониторинга приложений
- Контроль устройств
- Контроль системы
- Автоматическая блокировка эксплойтов

UserGate

- ПАК
- Фильтрация почты
- Балансировка нагрузки
- Гостевой доступ
- Поддержка удаленного доступа

Solar webProxy

- ПО или ПАК
- Аутентификация и авторизация
- Анализ трафика
- Обратное проксирование
- Очистка входящего трафика
- МЭ + NAT

Ideco UTM

- ПАК
- МЭ + СПВ
- Контроль приложений
- Анализ и очистка трафика
- VPN
- Удаленный доступ

Zecurion SWG

- Программный комплекс

- Контроль доступа
- Идентификация и аутентификация
- Безопасность облачных сервисов
- Интеграция с DLP
- Соответствие отраслевым стандартам

КРИПТОШЛЮЗЫ

Криптошлюз (криптографический шлюз, vpn-шлюз, криптомаршрутизатор) — аппаратно-программный комплекс криптографической защиты трафика данных, голоса, видео на основе шифрования пакетов по протоколам IPsec AH и/или IPsec ESP при установлении соединения, соответствующий требованиям к средствам криптографической защиты информации

Криптошлюз предназначен для обеспечения информационной безопасности организации, защиты её информационных сетей от вторжения со стороны сетей передачи данных (Интернет), обеспечения конфиденциальности при передаче информации по открытым каналам связи (VPN), а также организации безопасного доступа пользователей к ресурсам сетей общего пользования.

Криптошлюз обеспечивает базовую функциональность современного VPN-устройства:

конфиденциальность и целостность потока IP-пакетов;

маскировку топологии сети за счет инкапсуляции трафика в защищённый туннель;

прозрачность для NAT;

аутентификацию узлов сети и пользователей;

унификацию политики безопасности для мобильных и «внутренних» пользователей (динамическое конфигурирование корпоративных IP-адресов для удаленных пользователей «внутри VPN»).

Криптошлюзы представлены как в сегменте VPN устройств, так и в сегменте унифицированных устройств (UTM) объединяющих несколько средств безопасности в одном.

Отличие криптошлюзов от обычных VPN маршрутизаторов заключается в том, что они работают на основе протокола IPSec и обеспечивают защиту информации, передаваемой по каналам связи, используя алгоритмы, которые отвечают требованиям криптографических стандартов

ДОСТУП К РЕСУРСАМ ИНФОРМАЦИОННОЙ СИСТЕМЫ

Криптошлюзы позволяют осуществить защищённый доступ удаленных абонентов к ресурсам корпоративной информационной системы. Доступ производится с использованием специального программного обеспечения, установленным на компьютере пользователя (VPN-клиент) для осуществления защищённого взаимодействия удаленных и мобильных пользователей с криптошлюзом.

Программное обеспечение криптошлюза (сервер доступа) проводит идентификацию и аутентификацию пользователя и осуществляет его связь с ресурсами защищаемой сети. С помощью криптошлюзов формируют виртуальные защищённые каналы в сетях общего пользования (например, Internet), которые гарантируют конфиденциальность и достоверность информации, и организовывать виртуальные частные сети (Virtual Private Network – VPN), представляющие собой объединение локальных сетей или отдельных компьютеров, подключенных к сети общего пользования в единую защищённую виртуальную сеть. Для управления такой сетью обычно используется специальное программное обеспечение (центр управления), которое обеспечивает централизованное управление локальными политиками безопасности VPN-клиентов и криптошлюзов, рассылает для них ключевую информацию и новые конфигурационные данные, обеспечивает ведение системных журналов.

Diamond VPN/FW

- Пропускная до 20 Гбит/с
- МЭ
- СОВ
- СПВ
- Масштабирование

Diamond VPN/FW

Dionis-NX

- Пропускная до 10 Гбит/с
- VPN

Dionis-NX

ViPNet Coordinator HW4 (5)

- Пропускная зависит от исполнения
- МЭ
- Фильтрация трафика

ViPNet Coordinator HW4 (5)

Континент 3.9

- Пропускная зависит от исполнения
- Аппаратное криптоускорение

КОД безопасности

Континент 3.9

С-Терра Шлюз

- Пропускная зависит от исполнения

С-Терра Шлюз


LAN3
LAN2
LAN1
USB3.0
s-terra
RESET
USB3.0
HDMI
CONSOLE
DC Jack

ФПСУ-IP

- Пропускная до 12 Гбит/с
- резервирование для VPN-сетей

АМИКОН

ФПСУ-IP

Заключение

- В настоящий момент сетевая безопасность является одним из ключевых вопросов при планировании и реализации сетевой инфраструктуры; неудачное решение может существенно понизить надежность сетевой инфраструктуры
- При построении безопасных сетей используется множество аппаратно-программных решений, среди наиболее часто используемых – виртуальные частные сети и пакетные фильтры.